NA HRVATSKOM JEZIKU!

Praktični vodič za siguran rad na Internetu kod kuće

Sigurni na Internetu

Andrew Conry-Murray i Vincent Weafer

Od proizvođača programa

Norton AntiVirus™

MIŠ

Praktični vodič za siguran rad na Internetu kod kuće

Sigurni na Internetu

Andrew Conry-Murray i Vincent Weafer

MIŠ

Naslov izvornika
Andrew Conry-Murray i Vincent Weafer
The Symantec Guide to
Home Internet Security

Copyright © 2006 Symantec Corporation

Copyright © za hrvatsko izdanje MIŠ d.o.o., 2005.

Sva prava pridržana. Ni jedan dio ove knjige ne smije se reproducirati ili prenositi u bilo kojem obliku, ni na bilo koji način, elektronski ili mehanički, uključujući fotokopiranje, snimanje ili pohranjivanje u bazu podataka bez odobrenja nakladnika.

U vezi s primjenom ovdje sadržanih obavijesti ne pretpostavlja se obveza patentiranja. Premda su izdavač i autori vrlo pomno priredili ovu knjigu, ne prihvaćaju odgovornost za pogreške i propuste ni obveze u vezi s mogućom štetom nastalom primjenom ovdje sadržanih informacija.

ZAŠTITNI ZNAKOVI
Svi pojmovi spomenuti u ovoj knjizi za koje se zna da su zaštitni znakovi ili službene oznake na odgovarajući su način napisani velikim slovima. Izdavač ne može provjeriti točnost tih podataka. Primjena pojma u ovoj knjizi ne bi se smjela smatrati utjecanjem na vjerodostojnost zaštitnog znaka ili službene oznake.

UPOZORENJE I OGRAĐIVANJE
Najveći mogući trud uložen je da bi ova knjiga bila što potpunija i točnija, ali to ne podrazumijeva nikakvo jamstvo ili obvezu. Autori i izdavač nemaju obvezu ni odgovornost prema bilo kojoj osobi ili entitetu u vezi s ikakvom štetom ili gubitkom zbog informacija sadržanih u ovoj knjizi.

Authorized translation from the English language edition, entitled SYMANTEC GUIDE TO HOME INTERNET SECURITY, THE, 1st Edition by CONRY-MURRAY, ANDREW; WEAFER, VINCENT, published by Pearson Education, Inc, publishing as Addison Wesley Professional, Copyright © 2006 Symantec Corporation.

All rights reserved. No part of this book may be reproducted or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage retrieval system, without permission from Pearson Education, Inc.

CROATION language edition published by MIS D.O.O., Copyright © 2005.

MIŠ d.o.o.
Zagreb, Nova cesta 136 a

Za nakladnika
Snježana Sremić

Prevela s engleskoga
Andreja Prevarek

Korigirala
Rada Fedor

Redigirali
servis računala
Alba Avis
www.alba-avis.hr

Priprema za tisak
Grafički studio MIŠ

Tisak
Tiskara Zelina, 2005.

ISBN 953-6961-68-7

www.mis.hr

Sadržaj

Zahvale

O autorima

Uvod

1. poglavlje **Opasnosti koje prijete na Internetu** 1

1.1 **Prevaranti i otmičari** 2

Krađa identiteta 3

Spam 3

Virusi i crvi 4

Spyware, *adware* i trojanski konji 4

1.2 **Zašto baš ja?** 5

Vaše računalo je resurs za napade na druga računala 5

Vaše računalo komunikacijsko je sredstvo prevaranata 6

2. poglavlje **Sprječavanje krađe identiteta** 9

2.1 **Kako se kradu identiteti?** 10

Društveni inženjering 11

Spoofing 12

Phishing napadi 12

Keystroke loggeri 13

Krađa pošte i kopanje po smeću 14

2.2 **Sprječavanje krađe identiteta** 14

Razmislite prije nego što kliknete 14

Alati koji vam pomažu u sprječavanju krađe identiteta 15

SSL 16

Sigurnosni tokeni 17
SpoofStick 18
2.3 Oporavak od krađe identiteta 19
2.4 Popis za provjeru 20
Učinite 20
Nemojte učiniti 21
2.5 Korisni izvori 21

3. poglavlje Vatrozidovi 27
3.1 Paketi, protokoli i portovi 28
IP i TCP 29
HTTP i HTML 30
3.2 Što vatrozidovi mogu učiniti? 31
Regulirajte ulazne i izlazne veze 31
Postavke sigurnosti 33
3.3 Što vatrozidovi ne mogu učiniti? 35
3.4 Besplatni vatrozidovi 36
Windows XP Service Pack 2 36
ZoneAlarm iz ZoneLabsa 39
3.5 Vatrozidovi koje možete kupiti 41
Kako valja birati? 43
3.6 Testiranje vatrozidova 44
ShieldsUP! (www.grc.com) 44
Symantec Security Check (www.symantec.com/homecomputing/) 44
McAfee MySecurityStatus (http://us.mcafee.com/MySecurityStatus/) 44
PivX PreView (www.pivx.com/preview) 45
AuditMyPC (www.auditmypc.com) 45
3.7 Popis za provjeru 45
Učinite 46
Nemojte učiniti 46
3.8 Korisni izvori 46

4. poglavlje Kako se riješiti nepoželjnih gostiju? 1. dio: virusi i crvi 47
4.1 Porast malwarea 47
4.2 Virusi i crvi 50
Što crvi i virusi mogu učiniti? 53
4.3 Antivirusni softver 54
Što AV softver može učiniti? 54
Što AV softver ne može učiniti? 54
4.4 Ostale metode zaštite 56
Upotrijebite vatrozid 56

Ne otvarajte neobične poruke e-pošte 57
Nemojte kliknuti na veze ili programe unutar poruka e-pošte 58
Ažurirajte svoj softver 58
4.5 Što učiniti ako imate virus ili crva 59
Kako vidjeti je li računalo zaraženo? 59
Kako ukloniti virus ili crva? 59
4.6 Kako odabrati neki antivirusni proizvod? 60
4.7 Popis za provjeru 62
Učinite 62
Nemojte učiniti 62
4.8 Korisni izvori 62

5. poglavlje Kako se riješiti nepoželjnih gostiju? 2. dio: *spyware*, *adware* i trojanski konji 67

5.1 Što su *spyware*, *adware* i trojanski konji? 67
Definiranje *spywarea* i *adwarea* 69
5.2 Tehnički i zakonski izazovi otkrivanja i uklanjanja *spywarea* i *adwarea* 72
Želite li kolačić? 78
5.3 Kako *spyware/adware* i trojanski konji inficiraju vaše računalo 80
Iz Web pretraživača 80
Iz drugog softvera 81
Iz e-pošte 82
Iz društvenog inženjeringa 82
5.4 Kako se zaštiti od *spywarea*, *adwarea* i trojanskih konja? 82
Koristite *anti-spyware* i antivirusni softver 82
Pazite na oportuniste 85
Besplatan *anti-spyware* softver 86
Što može *anti-spyware* softver? 87
Što *anti-spyware* ne može? 88
Budite oprezni s besplatnim softverom 88
Pročitajte EULA-u 89
Podesite postavke svojeg pretraživača 89
Koristite neki alternativni pretraživač 91
Stalno ažurirajte svoj softver 91
5.5 Kako ukloniti *spyware*, *adware* i trojanske konje? 92
Kako prepoznati zaraženo računalo? 92
Korištenje alata HijackThis 93
Preformatiranje tvrdog diska 95
5.6 Popis za provjeru 95
Učinite 95
Nemojte učiniti 95
5.7 Korisni izvori 96

6. poglavlje **Recite 'ne' *spamu*** 99
6.1 *Spamonomija* 101
6.2 *Spam, scamovi* i *phishing* 102
6.3 Kako rade *spameri*? 104
Kupovanje popisa 104
Strvinari e-pošte 104
Napad po rječniku/žetva imenika 104
Krivotvorenje 105
Spam proxyji 105
Društveni inženjering 106
Web signali/Web bugovi 106
6.4 Metode za filtriranje *spama* 106
Filtri sadržaja/pretraživanja po ključnoj riječi 107
Crne liste 108
Bijele liste 108
Heurističke analize 108
Potpisi *spama* 109
Izazov/odgovor 110
Bayesiansko filtriranje 110
Filtriranje reputacije 111
6.5 Kako reducirati *spam*? 112
Izbrišite sumnjive poruke e-pošte bez otvaranja 112
Ne odgovarajte na spam ili phishing poruke 113
U porukama kojima ne vjerujete ne klikajte na veze 113
Čitajte izjave o privatnosti 113
Ne šaljite svoju adresu e-pošte 113
Promijenite svoju adresu e-pošte ili koristite nekoliko adresa 114
Ne kupujte ništa od spamera 115
Izvijestite o spamu i phishingu 115
6.6 *Anti-spam* alati 116
6.7 Popis za provjeru 118
Učinite 118
Nemojte učiniti 118
6.8 Korisni izvori 118

7. poglavlje **Osiguravanje Windowsa** 119
7.1 Windows XP Service Pack 2 121
Windows Security Center 121
Konfiguriranje Windows Firewalla 124
Zaštita od virusa 127
Zaštita od prelijevanja međumemorije 128
7.2 Utorci zakrpa 128
Uključivanje opcije Automatic Updates 130

7.3 Osiguravanje Internet Explorera 131
Sigurnost Internet Explorera 132
Rad s ActiveXom 132
Konfiguracija privatnosti 136
Pop-Up Blocker 138
7.4 Alternativni pretraživači 139
Firefox (www.mozilla.org) 140
Opera (www.opera.com) 141
7.5 Provjere sigurnosti 142
ShieldsUP! (www.grc.com) 142
PivX PreView (www.pivx.com/preview) 142
Symantec Security Check (www.symantec.com/securitycheck/) 143
7.6 Internet Explorer 7.0 i Windows Vista (Longhorn) 143
7.7 Popis za provjeru 144
Učinite 144
Nemojte učiniti 144
7.8 Korisni izvori 144

8. poglavlje Sigurnost vaše obitelji na Internetu 147
8.1 Filtriranje nepoželjnog sadržaja 148
Ljudski nadzor 149
Filtriranje tražilice 151
Filtriranje Internet Explorera 153
Filtriranje alternativnih pretraživača 158
Kontrole davatelja usluga 158
Kontrola spama 159
8.2 Seksualni grabežljivci i Internet 160
Sprječavanje nepoželjnih kontakata 161
Prijava seksualnih mamljenja 162
Softver za nadziranje Interneta 162
Kako valja birati? 163
8.3 Pjesma od 3.000 USD i drugi problemi s dijeljenjem datoteka 164
Kako me mogu uloviti? 168
Problemi sigurnosti kod P2P mreža 168
Legalno ili ilegalno? 169
8.4 Popis za provjeru 170
Učinite 170
Nemojte učiniti 170
8.5 Korisni izvori 170

9. poglavlje Bežična i VoIP sigurnost 173
9.1 Kako radi bežična mreža? 174

9.2 Sigurnosti kod kućnih WLAN-ova 175
Promjena osnovnog SSID-a 180
Isključite emitiranje 180
Promijenite osnovne lozinke 180
Uključite MAC filtriranje 180
Sigurnosni softver za bežične sustave 181
9.3 Sigurnost na javnim mjestima 182
Neosigurane vruće točke 183
Zli blizanac 185
Nemojte provoditi osjetljive transakcije na vrućoj točki 185
9.4 Sigurnost mobilnih telefona i osobnih digitalnih pomoćnika 185
Prijenosni operativni sustavi i Bluetooth 186
Malware mobilnih telefona 187
Osiguravanje Bluetootha 188
Sigurnost PDA uređaja 189
9.5 VoIP sigurnost 190
VoIP i 112 191
9.6 Popis za provjeru 192
Učinite 192
Nemojte učiniti 192
9.7 Korisni izvori 192

10. poglavlje Privatnost i Internet 195
10.1 Opcije privatnosti na Internetu 197
Osnove šifriranja 197
Digitalni potpisi i digitalni certifikati 199
Šifriranje e-pošte 200
Šifriranje datoteka i mapa 203
Proizvodi za anonimnost na Webu 204
10.2 Kako postupati s mešetarima podataka 205
Acxiom (www.acxiom.com) 206
ChoicePoint (www.choicepoint.com) 206
10.3 Popis za provjeru 207
Učinite 207
Nemojte učiniti 207
10.4 Korisni izvori 207

Zaključak 209

Kazalo 211

Rječnik 221

Zahvale

Najprije bih se želio zahvaliti svojoj supruzi Clare koja je zapravo postala samohrani roditelj usred pisanja svoje doktorske disertacije i poklonila mi vrijeme potrebno za pisanje ove knjige. Bez njezine ljubavi, podrške i poticanja ne bih je mogao napisati. Zahvaljujem svojem sinu Aidanu koji je žrtvovao mnoge priče i vrijeme za igru zbog ove knjige.

U Addison-Wesleyu zahvalio bih se Jessici Goldstein za njezin entuzijazam kod vođenja ovog projekta i Franku Vellai za brigu o svim detaljima. Zahvalio bih se Jessici i Franki za vođenje novog autora kroz procese izdavanja i izdavačke ugovore. Isto tako, zahvaljujem se Audrey Doyle i Gayle Johnson za njihove oštre uredničke oči i konstruktivne komentare.

U Symantecu bih se zahvalio Lindi McCarthy za ovu sjajnu priliku te Vincentu Weaferu za njegovu tehnološku ekspertizu, dubinsko poznavanje sigurnosti i naporan rad – naročito njegovoj sposobnosti kopanja po zamršenim stvarima koje okružuju spyware i iznalaženja jasnih definicija.

Želim zahvaliti i svojim kolegama, prijašnjim i sadašnjim iz *Network Magazinea/IT Architecta.* Posebno Steveu Steinkeu i Elizabeth Clark koji su mi omogućili da počnem raditi kao urednik i pisac i pustili me da zagrizem u sigurnost. Zahvaljujem se i Artu Wittmannu, Andy Dornan, Nancy Hung, Davidu Greenfieldu, Dougu Allenu, Haigu MacGregoru i Johnu Angelu. Svi su mi oni pomogli da naučim sva čuda mrežnih i računalnih tehnologija i pokazali mi kako postati bolji pisac, i primjerom i vrhunskim (iako ne uvijek ljubazno primljenim) kritikama.

I na kraju želim se zahvaliti svojim roditeljima, svojoj sestri i klanovima Ouellettea, Murraya, Conryja i Smithova za svaki pruženi oblik ljubavi i podrške uključujući (ali ne ograničavajući se samo na to) intelektualne poticaje, novac, smještaj, glazbu, brigu i gostoljubivost.

Andrew Conry-Murray

Zahvaljujem se Andrewu za cijeli njegov naporan rad i predanost ovoj knjizi i za njegovo beskrajno strpljenje s mnogim promjenama na koje smo nailazili. Želim se zahvaliti i timu u Symantecu na pomoći u revidiranju ove knjige te "brušenju" poruka u njoj kako bi one postale jasnije i razumljivije. Posebno se zahvaljujem Jessici i Franku iz Addison-Wesleya i Lyndi McCarthy iz Symanteca koji su nas stalno vodili pravim putem. Osobno, želim zahvaliti svojoj supruzi Caitrioni i obitelji – Davidu, Sineadu i Roghanu – jer su uz mene probdjeli mnoge noći u radu na sigurnosnim incidentima od kojih se gradilo iskustvo za ovu knjigu.

Vincent Weafer

O autorima

Andrew Conry-Murray je urednik za tehnologiju u IT Architectu, časopisu za IT profesionalce koji je osvojio brojne nagrade. Andrew piše članke o računalima i sigurnosti na mreži od 2000. godine.

Vincent Weafer ima opsežno iskustvo koje je stekao tijekom 20 godina rada u informatičkoj industriji na poslovima od razvoja softvera do sistemskog inženjeringa i istraživanja sigurnosti. Posljednjih je osam godina operativni vođa Symantec Global Security Response tima, gdje mu je misija proširiti istraživanja na nove prijetnje za sigurnost računala te ponuditi sadržajna rješenja kao što su antivirusna, anti-spam rješenja, odgovori na provale i ranjivost, upozoravanje u realnom vremenu, istraživanja i analize.

Weafer je i jedan od Symantecovih glavnih glasnogovornika o prijetnjama i trendovima za sigurnost na Internetu, za američki tisak, radio i televiziju, a pojavljuje se na CBS-u, ABC-u, NBC-u, CNN-u i BBC-u uz mnoge druge kanale. Uz to je održao predavanja na brojnim konferencijima o prijetnjama i trendovima sigurnosti, te pisao članke i davao svoj doprinos tehničkim panel diskusijama koje, između ostalih, vode European Institute for Computer AntiVirus Research (EICAR), Virus Bulletin, Association of AntiVirus Asia Researchers (AVAR) i Australian Computer Emergency Response Team (AUSCERT).

Uvod

Hvala vam što ste odabrali ovu knjigu. Ako tražite brza i jednostavna rješenja da biste svoje Windows-temeljeno računalo održavali sigurnim od tamne strane Interneta onda je to to! Ova je knjiga posebno namijenjena "tehnički nestručnim" korisnicima, pa sadrži ugodne postepene upute i korisne slike. Ako znate kako *surfati* Webom i preuzimati softver s Interneta, tada imate dovoljno znanja potrebnog da biste stekli novo o sigurnom druženju s Internetom.

Danas sve više i više ljudi provodi osjetljive transakcije putem e-pošte i Interneta, kao što su online bankarstvo, trgovina dionicama, e-trgovina i upravljanje osobnim računima. Iako su sada pomoću Interneta te aktivnosti jednostavnije, Internet nas izlaže i sigurnosnim rizicima. Tradicionalni rizici kao što su virusi, crvi i trojanski konji i dalje preplavljuju Internet. Uz to, nove se prijetnje pojavljuju, uključujući *spyware*, Internetske prijevare i *spam*. Te prijetnje koje pune naslove u novinama i kojima se bave kriminalci motivirani profitom, postale su nevjerojatno sofisticirane, imaju kraći životni ciklus i koriste nove načine širenja zaraze. Te prijetnje uzrokuju nove glavobolje svakome tko koristi Internet.

Čak i naoko sigurne informativne i zabavne lokacije mogu donijeti rizike. Na primjer, u studiji koju je provela tvrtka za sigurnost na Internetu, Symantec, istraživači su uzeli potpuno novi Windows PC, spojili ga na Internet bez ikakvog zaštitnog softvera i pretražili Web. Proveli su jedan sat u interakciji s različitim kategorijama Web lokacija, uključujući lokacije za e-trgovinu, kockanje i nove lokacije. Iznenađujuće, dječje su Web lokacije iskrcale najnepoželjniji softver na testni PC – 359 *adwarea* (softvera koji generira iskočne oglase) u samo jednom satu surfanja!

Primarni cilj ove knjige jest pomoći vam da razumijete kako korištenje Internet nosi određenu dozu rizika – za vašu privatnost, integritet i upotrebljivost vaših osobnih podataka te performanse vašeg računala. Ovdje jasno objašnjavamo te rizike i pokazujemo vam na jednostavan ali detaljan način kako smanjiti vlastitu izloženost.

Za razliku od drugih knjiga o sigurnosti koje se fokusiraju na jedan ili dva problema kao što su primjerice, virusi ili *spam*, namjena ove knjige je da bude opsežan vodič za široki raspon rizika s kojima se suočavaju korisnici Interneta. Tu ćete pronaći bogate informacije o tome kako svoje Windows računalo održati slobodnim od *spywarea*, crva, virusa, *spama* i provalnika; kako sigurno koristiti e-poštu i Web pretraživač; kako zaštititi svoj identitet i privatnost, kako zaštititi bežičnu vezu od njuškala i *scamera* te kako svoju djecu držati podalje od pornografije i *online* grabežljivaca.

Prođete li površno po poglavljima ili ako pregledate sadržaj, uvidjet ćete da ova knjiga obuhvaća mnogo detalja – uključujući i postepene upute – o tome kako odabrati i koristiti sigurnosni softver iz vrlo bogate ponude, kako iskoristiti sigurnosne značajke ugrađene u Windows XP Service Pack 2 i kako sebe i svoju obitelj zaštititi od kriminalaca i prevaranata da ne postanete njihovim žrtvama. Mnogi su softverski alati i programi koje ovdje preporučujemo besplatni.

Ova je knjiga napisana tako da vam pomogne u rješavanju specifičnih problema, pa je ne morate pročitati od korica do korica. Možete jednostavno početi s bilo kojem poglavljem u kojem se nalazi ono što vas trenutno najviše brine i dobit ćete potrebne informacije. Naravno, rizici na Internetu često su isprepleteni, pa se zato u knjizi nalaze reference na druga relevantna poglavlja.

Internet se često uspoređuje sa super-autocestom, ali on više sliči velikom gradu – u kojem provodimo sve više i više vremena. To je i grad gotovo beskonačne veličine i ozbiljnih opasnosti. Ova je knjiga zato napisana tako da predstavlja pouzdani vodič kroz taj grad kako biste vi i vaša obitelj mogli u njemu sigurno uživati.

1. poglavlje

Opasnosti koje prijete na Internetu

Pokušajte zamisliti život bez Interneta. U samo nekoliko kratkih godina ova je tehnologija postala nezamjenjiva; na nju se oslanjamo pri komuniciranju, zabavi, informiranju i trgovini. Internet i World Wide Web učinili su naše živote zabavnijima i produktivnijima.

Na žalost, Internet je postao nezamjenjiv i lopovima, vandalima te stručnjacima za otkrivanje tajnih podataka. Internet i Web su pod sve žešćim udarom kriminalaca koji moć globalne mreže koriste za uništavanje vaših datoteka, narušavanje vaše privatnosti, otimanje ili uništavanje računala, pa čak i za krađu vašeg novca i terećenje kreditnih kartica.

No, iako su rizici stvarni, mogu se izbjeći. Za to postoje brojni alati i tehnike, pa stoga ne trebate okrenuti leđa svemu što Internet pruža. A s ovom knjigom, kao svojim vodičem, nije potrebno ni da postanete stručnjak za sigurnost; ako ste ikada koristili neki Web pretraživač ili instalirali neki softver, tada imate znanje potrebno da zaštite sebe i svoju obitelj.

Problem sigurnosti na Internetu možete usporediti sa svojim automobilom. Svaki put kada ga vozite prihvaćate određene rizike: vaš se automobil može pokvariti, možete doživjeti prometnu nezgodu, pa čak i smrtno stradati. Te rizike prihvaćate zato jer vam je automobil neophodan. On ima kočnice, sigurnosne pojaseve i zračne jastuke. Vi ste pohađali auto-školu. Automobil ste osigurali.

Svaki put kada koristite Internet, također prihvaćate određene rizike: krađu identiteta, viruse, *spam*, *spyware* i tako dalje. Čak i naoko bezazlene lokacije poput popularnih odredišta za e-trgovinu ili *online* zabavu mogu preplaviti vaše računalo softverom koji generira oglašavanje (i usporava rad vašeg PC-ja) ili prati vaše korištenje Interneta. Velik je broj korisnika koji, međutim, koriste Internet ne poduzimajući nikakve korake za ublažavanje rizika: nemaju vatrozid, ni antivirusni softver, ni ikakve ideje o tome da prevaranti i otmičari aktivno "plaze" Internetom u potrazi za novim žrtvama. To je poput upravljanja automobilom bez kočnica i sigurnosnih pojaseva. Ovom knjigom želimo vam pomoći razumjeti rizike koje Internet skriva i pružiti informacije potrebne da biste uklonili te prijetnje.

Ovo poglavlje sadrži pregled najžešćih rizika na Internetu i objašnjenja zašto su kućni PC-ji toliko privlačne mete Internet kriminalcima. No, imajte na umu da, pored izloženosti aktivnostima kriminalaca, korištenje Interneta također predstavlja prijetnju vašoj obitelji omogućavajući pristup nepoželjnim sadržajima poput pornografije ili aktivnostima kao što su *online* kockanje i ilegalno širenje autorskim pravima zaštićene glazbe i filmova. Nezaštićene bežične kućne mreže ili javne bežične vruće točke također mogu izložiti vaše privatne informacije svakome tko posjeduje prijenosno računalo s bežičnim pristupom Internetu. Te ćemo probleme objasniti poglavljima koja slijede.

1.1 Prevaranti i otmičari

Napadi na kućne korisnike spadaju u dvije osnovne klase: prijevaru i otmicu. Računalna prijevara je pokušaj izmamljivanja novca nuđenjem sumnjivih proizvoda e-poštom i iskočnim oglasima, ili pak navođenje na otkrivanje osobnih informacija ili podataka o bankovnim računima (primjerice lozinke ili brojeva računa). Krađa identiteta, *phishing* i *spam* najbolji su primjeri računalne prijevare.

Otmičari pokušavaju preuzeti kontrolu nad vašim računalom kako bi proveli svoje zle namjere poput praćenja vaše *online* aktivnosti, prikazivanja neželjenih oglasa, slabljenja performansi vašeg računala ili veze s Internetom, ili pak "regrutiranja" vašeg računala za slanje *spama* i napadanje drugih meta na Internetu.

Kriminalci se pri otimanju računala snažno oslanjaju na *malware* (softverski programi koji se koriste iskučivo zlonamjerno). *Malware* obuhvaća viruse, crve, trojanske konje, spyware i *adware*. U nekim slučajevima kriminalci kombiniraju prijevare i otmice da bi ostvarili svoje ciljeve. Ovdje objašnjavamo koje su najčešće prijetnje s Interneta.

Krađa identiteta

Jedna od danas najvećih i najbrže rastućih prijetnji s Interneta je krađa identiteta – kopiranje informacija poput brojeva kreditnih računa, lozinki i osobnih matičnih brojeva. Te se informacije mogu koristiti za *online* ili *offline* prijevare.

Prema podacima Federalne trgovinske komisije SAD-a (*Federal Trade Comission*), gotovo je 10 milijuna Amerikanaca bilo žrtvama krađa identiteta 2003. godine. U ekstremnim slučajevima, financijski gubici kreću se i do nekoliko desetaka tisuća američkih dolara. Žrtvama je često narušen i kreditni rejting, a da bi se on obnovio treba proći i nekoliko mjeseci.

Phishing napadi su oblik krađe identiteta prijevarom koji se oslanja na e-poštu i Web. Evo kako se to dogodi. Dobivate poruku e-pošte u kojoj se tvrdi da dolazi iz neke velike banke, kompanije za izdavanje kreditnih kartica ili s neke lokacije za e-trgovinu. U poruci piše da postoji problem s vašim računom i mole vas da pošaljete svoje korisničko ime, broj računa i lozinku kako biste potvrdili status svojeg računa. Međutim, ta je poruka e-pošte lažna. Ako odgovorite na nju, zapravo otkrivate svoje povjerljive podatke prevarantima, vjerojatno s nekog drugog kontinenta, ili barem iz druge zemlje.

Unaprijeđena verzija ove prijevare uključuje hipervezu u poruci e-pošte. Kliknete li na tu vezu vidjet ćete stranicu za prijavu koja izgleda identično stranici za prijavu vaše banke, kompanije za izdavanje kreditnih kartica ili Web lokacije za e-trgovinu, uključujući i odgovarajući logotip. Nakon što upišete tražene podatke dobit ćete poruku o pogrešci i vjerojatno će vas zamoliti da ponovite unos istih informacija. U međuvremenu, informacije za prijavu šalju se na neki poslužitelj pod kontrolom vještih prevaranata. Oni te informacije koriste za kupnju ili podizanje novca u vaše ime. A isto tako mogu i prodavati te ukradene informacije drugim kriminalcima.

Spam

Prema nekim procjenama, neželjene poruke e-pošte (poznatije kao *spam*) sada predstavljaju gotovo 80% cjelokupnog prometa e-pošte na Internetu. Iako *spam* u smislu štete nije tako značajna prijetnja kao *malware* ili krađa identiteta, on je zasigurno jedan od najgorih napasti s Interneta. Da biste izbrisali neželjene poruke e-pošte gubite vrijeme, a poruke često sadrže uvredljiv sadržaj ili slike. Kradljivci identiteta često koriste *spam* tehnike za slanje lažnih poruka.

Virusi i crvi

Virus je samoreplicirajući kôd koji živi unutar tijela domaćina, poput primjerice Wordova dokumenta. Crv je samoreplicirajući program koji se prenosi s računala na računalo. Crvi i virusi često sadrže zlonamjerni programski sadržaj (*payload*) koji može preuzeti kontrolu nad računalom, uništiti datoteke na njemu ili ukrasti osobne podatke. Istraživanje pokazuje da se na Internetu tjedno pojavljuje 500 novih virusa i crva. Svake godine broj virusa i crva raste za 400%, a kriminalci na Internetu postaju sve vještiji pri kreiranju brzo širećih crva. Na primjer, 2004. godine crv Blaster zarazio je 100.000 računala u samo pet sati. Jedan još brži crv, SQL Slammer, toliko se brzo razmnožava da se broj računala koja je zarazio udvostručavao svakih 8,5 sekundi tijekom prve minute njegova postojanja.

Spyware, *adware* i trojanski konji

Spyware je još jedna rastuća kategorija *malwarea*. Pojam "spyware" često se koristi kao općenit opis za skup programa raznih sposobnosti, poput mijenjanja telefonskog broja koji bira vaš modem prilikom spajanja na Internet, nadziranja i prikupljanja podataka o pritisnutim tipkama ili preusmjeravanja vašeg pretraživača na neželjene Web lokacije.

Adware je zasebna, ali bliska vrsta programa. *Adware* skuplja informacije o vama i vašim navikama *surfanja* po Webu koje se koriste za ciljano oglašavanje. *Adware* programi mogu ispuniti vaš ekran iskočnim oglasima, preusmjeriti vas na čudne stranice za pretraživanje i znatno oslabjeti performanse vašeg računala.

Za razliku od virusa i crva, *spyware* i *adware* ne repliciraju sami sebe. Ti se programi nastanjuju na vašem računalu bez vašeg znanja. To se može dogoditi prilikom posjeta nekoj Web stranici koja potajice učita program na računalo. *Spyware* i *adware* mogu doći i u paketu s besplatnim pomoćnim programima poput screen savera, programa za praćenje vremenske prognoze i alatnih traka pretraživača. Softver koji vam omogućuje dijeljenje glazbenih i video-datoteka trajan je izvor *adwarea*. Prema istraživanjima Earthlinka, prosječno kućno računalo ima u sebi 25 *spyware* i *adware* programa.

Zatim su tu i *trojanski konji*. Ti su softverski programi dobili ime prema legendi o Trojanskom konju u kojeg su se grčki vojnici sakrili da bi se uvukli u dobro utvrđen grad Troju. Kada se konj našao iza zidina grada, grčki su vojnici pričekali noć, a zatim izašli van i trojanske vojnike pobili na spavanju te zauzeli grad.

Današnji trojanski konji neće vas ubiti na spavanju, ali zato udaljenom napadaču mogu pružiti potpunu kontrolu nad vašim računalom. Napadač tada može čitati, mijenjati i brisati vaše datoteke; pokretati programe, instalirati ili uklanjati softver i općenito vas učiniti bespomoćnim i jadnim što se računala tiče.

1.2 Zašto baš ja?

Pogrešno je misliti kako ste zaštićeni od internetskog kriminala, čak i ako na svojem računalu imate samo slike s godišnjeg odmora, neke preuzete MP3 datoteke, nekoliko radnih dokumenata i svoj tajni dnevnik. Iako je istina da sadržaj tvrdih diskova pojedinaca nije zanimljiv zločestim dečkima, privlačnost za kriminalce s Interneta samo je jedna od karika: oni ne napadaju samo vas; oni napadaju istodobno tisuće ili stotine tisuća tuđih računala.

Količina je važna iz dva razloga. Prvi; kompromitirana računala i sama postaju resurs za napade na još više računala. Drugi; što je više potencijalnih žrtava koje prevaranti mogu doseći, to je veća mogućnost da neke upadnu u zamku. Razmotrimo pojedinačno ove ideje.

Vaše računalo je resurs za napade na druga računala

Vaš PC i njegova veza s Internetom vrijedne su mete jer u kombinaciji sa stotinama ili tisućama drugih postaju oružje koje napadači koriste protiv nekog trećeg – najčešće su to tvrtke ili vlade. Automatizirani softverski alati skeniraju široka područja Interneta u potrazi za ranjivim strojevima. Potom za nedopušten ulazak potom stalno iznova koriste istu metodu instalirajući zlonamjerne programe koji napadačima omogućuju upravljanje na daljinu tom vojskom strojeva. Ta oteta računala često se nazivaju "zombiji" ili "larve".

Kriminalci s Interneta koriste zombije na mnogo načina. Prvi; napadači koriste velik broj zombija za lansiranje denial-of-service (odbijanje usluge), ili skraćeno DoS, napada. DoS napadi sastoje se od odašiljanja velike količine mrežnog prometa na cilj, poput Web lokacija tvrtki ili vlade. Dovoljno veliki DoS napadi mogu ciljanu lokaciju izbaciti *offline*.

Kriminalci s Interneta koriste DoS napade i za iznuđivanje na Internetu: vlasnicima Web lokacija se prijeti napadom te ih se traži da daju novac ili će njihova Web lokacija biti ugašena. Takve su prijevare često učinkovite ako ciljane lokacije nisu sklone zatražiti pomoć ili osiguranje od zakonskih tijela. Pornografske lokacije, lokacije za kockanje i druge slične lokacije primarne su mete za ovu vrstu napada.

Drugi pak softver može pretvoriti vaše računalo u stroj za širenje *spama*. Širenje *spama* je postalo operacija vrste udari-i-bježi. *Spameri* stalno traže nova računala s kojih će slati svoju nepozvanu poštu jer su davatelji Internet usluga (Internet Service Providers – ISP-ovi) i anti-*spam* organizacije brzi u otkrivanju i blokiranju svakog računala koje šalje takvu poštu. Jedan trik *spamera* je da provale u kućna računala i koriste ih za slanje tisuća ili milijuna poruka, pa onda kreću dalje. Vaš problem je to što *vaša* e-pošta neće biti isporučena jer će vaše računalo biti obilježeno kao izvor *spama* i zato blokirano.

Neke grupe, uključujući i one organiziranog kriminala održavaju velike 'farme' kompromitiranih računala. One unajmljuju te otete strojeve najboljem ponuđaču koji će ih koristiti za lansiranje DoS napada ili slanje *spama*. Računala velikih brzina sa stalnom vezom na Internet osobito su vrijedna kriminalcima.

Posljednji je, ali ne i najmanje važan, dobar stari status. Virus ili crv koji se brzo širi svojem kreatoru ili kreatorima pribavlja publicitet. Što je više računala kompromitirano, veća su prava na hvalisanje.

Vaše računalo komunikacijsko je sredstvo prevaranata

U materijalnom svijetu prevaranti mogu u jednom trenutku pristupiti samo jednoj žrtvi. Na Internetu je broj potencijalnih žrtava gotovo beskonačan. Internet također olakšava kriminalcima skrivanje identiteta dok prijevarama dohvaćaju gotovo cijeli svijet.

E-pošta čini posao još lakšim, jer čak i dobro zaštićena računala prihvaćaju elektroničke poruke. Prijevare e-poštom, "pecanje" povjerljivih informacija i *spam* imaju nisku stopu povrata (samo 1 do 2 posto primatelja ovakvih poruka odgovara na njih) ali ako možete poslati stotine tisuća poruka (ili milijune poruka u slučaju *spama*) rezultat i dalje generira profit.

Jedna od popularnih prijevara e-poštom je ona kada prevaranti glume rođake bivših afričkih ministara naftne industrije. Ti "rođaci" traže pomoć u prebacivanju milijuna dolara iz zemlje, nudeći postotak od tog novca koji će uplatiti na vaš račun ako im pomognete. Sve što trebate učiniti je dati im broj svojeg bankovnog računa i možda poslati nekoliko tisuća dolara unaprijed da oni riješe "papirologiju".

Na nedavnom sam putu u Zapadnu Afriku stvarno vidio pet muškaraca u jednom *cybercafeu* kako šalju stotine takvih poruka, a svi su tvrdili da su supruga velike face iz svrgnute vlade. Pokušao sam jednog od njih intervjuirati jer bih tako dobio odličnu priču, ali on je isključio svoje računalo i odgovorio mi da je pisao prijateljima. Pa dobro! Imajte na umu da naftne kompanije u Africi nisu jedine meke:

Irak i zemlje bivšeg Sovjetskog Saveza također se koriste kao mamci, kao i zemlje koje su nedavno pretrpjele neku prirodnu katastrofu.

U drugoj varijanti ove sheme prevaranti glume žene iz Rusije. Oni počinju komunikaciju s muškarcima koji su na internetske servise za pronalaženje partnera poslali svoje profile. Daju fotografije (naravno, radi se o atraktivnim ženama) i uvlače žrtvu u opširnije dopisivanje. Uskoro "žena" priznaje svoju ljubav i izražava želju za sastankom. Slatka je dok posramljeno priznaje da je prisiljena tražiti novac za vizu, avionsku kartu ili nešto drugo. Na kraju, naivna žrtva izgubi stotine, pa čak i tisuće dolara.

Sljedeća poglavlja istražuju najbolje načine zaštite protiv ovih stalnih prijetnji s Interneta.

2. poglavlje

Sprječavanje krađe identiteta

Vaša sposobnost da dokažete svoj identitet – odnosno, moć uvjeravanja da ste stvarno osoba za koju se predstavljate – osnovni je način na koji se danas u svijetu provodi trgovina. Dokaze identiteta koristite da biste dokazali vlastitu autentičnost organizacijama s kojima poslujete ili da biste ovlastili isporuku usluga ili transakcija.

Na Internetu se vaš identitet sastoji od niza elemenata poput korisničkih imena, lozinki, osobnih identifikacijskih brojeva (PIN-ova), jedinstvenih matičnih brojeva, raznih brojeva računa i drugih osobnih podataka. Ti digitalni identiteti rade pod pretpostavkom da ste vi jedina osoba koja zna svoje podatke. To je loša pretpostavka i olakšava kriminalcima da počine zločin. Kada poslujete putem Interneta nitko od vas ne može tražiti vašu sliku da biste dokazali svoj identitet.

U ranim danima Interneta najgore što vam se moglo dogoditi, što se tiče krađe identiteta, bila je krađa korisničkog imena i lozinke koje ste koristili za svojeg davatelja Internet usluga (ISP-a), a to je značilo da je netko drugi mogao za vaš novac *surfati* Internetom.

Danas koristimo Internet za sve oblike financijskih transakcija, što bitno podiže ulog za krađu identiteta. Kriminalci mogu upotrijebiti vaš digitalni identitet za otvaranje računa kreditnih kartica, mijenjanje vaše adrese (da ne biste uočili čudne stavke u izvodima svojih računa kreditnih kartica), dizanje nenamjenskih i hipotekarnih kredita i provođenje financijskih transakcija, sve u vaše ime. Oni

ukradene identitete mogu prodavati drugim kriminalcima na dobro organiziranom crnom tržištu Interneta. Moguće posljedice velikog su raspona i sežu od uništenog kreditnog rejtinga do novca ukradenog s vašeg bankovnog računa.

Prijevara s kreditnim karticama najčešći je oblik krađe identiteta. Lopovi kradu osobne informacije i koriste ih za otvaranje računa u tuđe ime, troše po tom računu mjesec ili dva i potom jednostavno odbace karticu kada je kompanija koja ju je izdala blokira. Prema priči iz *New York Timesa*[1] jedan je lanac lopova za krađu identiteta ukrao preko 30.000 identiteta i zaradio milijune dolara tijekom dvogodišnjeg razdoblja, preprodajući robu kupljenu lažnim kreditnim karticama. Taj je lanac kriminalaca bio toliko uspješan jer je potkupio zaposlenika jedne kompanije koji je imao pristup digitalnim identitetima klijenata. Taj "interni" lopov zloupotrijebio je svoje ovlasti pristupa podacima te ukrao digitalne identitete i prodao ih bandi koja je otvorila lažne račune.

Profit se može ostvariti i od malog broja ukradenih identiteta. 2004. godine jedan je čovjek u Virginiji proglašen krivim za krađu imena i osobnih informacija desetoro ljudi. Te je informacije koristio za otvaranje kreditnih računa i kupnju robe u vrijednost od 85.000 američkih dolara koju je potom prodavao na eBayu.

Dok zločesti dečki kupuju ili nestaju s novcem od kredita, vas zatrpavaju računi. Čak i ako ne budete terećeni za te troškove, trebat ćete proći mukotrpan proces vraćanja kreditnog rejtinga u prethodno stanje.

Ovo poglavlje daje pregled načina na koje kriminalci mogu ukrasti vaš identitet i daje popis koraka koje trebate poduzeti da biste to spriječili, a osim toga daje vam i savjete kako se oporaviti ako je vaš identitet ukraden i zlorabljen.

2.1 Kako se kradu identiteti?

Postoje dva načina na koja se može ukrasti identitet. Jedan je način krađa informacija iz baza podataka banaka, ISP-ova, maloprodajnih mjesta, obračunskih ustanova i drugih entiteta koje pohranjuju takve informacije. Ponekad te informacije kradu vrlo vješti računalni kriminalci. Na primjer, u lipnju 2005. godine prijavljeno je da su računalni kriminalci ukrali informacije o računima za više od 200 000 kreditnih kartica iz kompanije za obradu naplate računa po kreditnim karticama, pod imenom CardSystem Solutions. Informacije o gotovo 40 milijuna kartica također su mogle biti otkrivene tijekom napada. Čest je slučaj da lopovima pomažu zaposlenici ili poslovni partneri koji imaju pristup podacima, kao

1 "Gone in 60 Seconds: Identitiy Theft is Epidemic. Can It Be Stopped?", Timothy L. O'Brien, *New York Times*, 24. listopad 2004. godine

što je bilo u slučaju objavljenom u proljeće 2005. godine u kojem su zaposlenici četiri velike banke prodali više od 670 000 zapisa o računima klijenata lopovima. I na kraju, informacije o identitetu mogu se dobiti preko dobrih staromodnih prijevara – *scamova*. U jednom nedavnom slučaju, lopovi su jednostavno glumili legitimne tvrtke da bi dobili pristup podacima o identitetu od obračunske ustanove pod imenom ChoicePoint. Umjesto izvršavanja složenog "hacka", lopovi su jednostavno nabavili kalifornijske licence za poslovanje a zatim kupili informacije o klijentima putem regularnih kanala od ChoicePointa. (Pojedinosti o tome kako se otkrila prijevara naći ćete na kraju ovog poglavlja.)

Kao računalni korisnik malo je toga što možete poduzeti da biste se zaštitili od ove vrste krađe identiteta, osim nadzirati svoje bankovne izvode i izvode kreditnih kartica ne biste li uočili čudne transakcije, stalno provjeravati svoj kreditni rejting i dobro paziti s kim ćete poslovati. U nekim slučajevima možete provjeriti jesu li podaci o vama pohranjeni u nekim obračunskim ustanovama. Detalje potražite u 10. poglavlju "Privatnost i Internet".

Drugi način krađe identiteta je da napadač izravno od vas ukrade informacije ili ih na prijevaru od vas dobije. U većini slučajeva lopovima je mnogo jednostavnije na ovaj način dobiti podatke nego provaljivati u dobro branjene mreže (iako upadanje u korporacijske baze podataka može biti uznemirujuće jednostavno za stručne i uporne provalnike, ali to je tema za neku drugu knjigu).

Kada se radi o drugom načinu krađe identiteta, u većini slučajeva možete nešto poduzeti. No, prije nego što vam objasnimo što zapravo, evo informacija o različitim načinima provala koje koriste kradljivci identiteta.

Društveni inženjering

Društveni inženjering maštovit je način upućivanja na – varanje ljudi. Društveni inženjering oslanja se na vaše prirođeno povjerenje u ljude (pa, dobro, lakovjernost) naročito u ljude koji imaju određene društvene uloge, poput onih u uniformama, sa iskaznicama ili u poslovnim odijelima.

Kriminalci i stručnjaci za sigurnost (koji se zovu i testeri za provale) koriste društveni inženjering kada pokušavaju provaliti na neku sigurnu lokaciju. Na primjer, testeri za provale u uredu nose odijelo i kravatu te se motaju naokolo da bi vidjeli što mogu pronaći. Rijetko itko posumnja u njihove namjere. Na primjer, jeste li ikada zatražili nepoznatog zaposlenika za identifikacijsku iskaznicu ako vas prati kroz vrata za koja morate koristiti karticu za otključavanje? Ako jeste, a on vam je odgovorio da ju je zaboravio na stolu, što ste tada učinili? Vrlo je vjerojatno da ste samo klimnuli glavom i propustili ga.

Vjerojatno najozloglašeniji društveni inženjer je Kevin Mitnick, osuđeni kriminalac koji svoja najsjajnija postignuća nije ostvario briljirajući svojim programerskim vještinama ili zahvaljujući torbi punoj računalnih trikova, već telefonom. Jedna od njegovih najdražih meta bile su telefonske kompanije. Nazvao bi telefonsku kompaniju i predstavio se kao inženjer te naveo osobu s druge strane linije da mu pruži sve vrste korisnih informacija, poput lozinki koju bi mu omogućile pristup osjetljivim računalnim sustavima. Više o Mitnickovim prijevarama i načinu na koji je uhvaćen možete pročitati u *Takedown: Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaw – By the Man Who Did It*, autora Tsutomua Shimomura i Johna Markoffa.

Brojne prijevare s namjerom krađe identiteta oslanjaju se do određenog stupnja na društveni inženjering. Najkorištenija sredstva su lažne poruke e-pošte koje ukazuju da dolaze iz zakonite organizacije ili bezazlene Internet lokacije koje nude besplatne sitnice poput softvera za razmjenjivanje datoteka, igrica ili pomoćnih programa koji sadrže i zlonamjerne programe za krađu povjerljivih informacija.

Spoofing

Internetski *spoofing* (podvaljivanje, krivotvorenje) znači kreiranje lažne ili krivotvorene verzije nečega, poput Web lokacije ili adrese e-pošte. Na primjer, mnogi kradljivci identiteta postavljaju lažne Web lokacije koje izgledaju isto kao i stvarne i navode korisnike na te lokacije. Kada se jednom nađe na odredištu, korisnik se prijavljuje sa svojim korisničkim imenom i lozinkom, koje tako dolaze u ruke kriminalcima, a oni ih zlorabe za pristup stvarnoj Web lokaciji. Ovo je poznato kao podvaljivanje Web lokacije – *Web site spoofing*. Spameri također podvaljuju povratnu adresu e-pošte, odnosno u svoju *spam* poruku uključuju povratnu adresu e-pošte koja zapravo ne postoji.

Phishing napadi

Phishing (pecački) napadi su najprominentniji i najštetniji napadi današnjih prevaranata s Interneta. Mnogi *phishing* napadi počinju porukom e-pošte. Na primjer, organizacija kriminalaca pošalje tisuće *spam* poruka koje ukazuju na to da ih je poslala banka, kompanija za izdavanje kreditnih kartica, ISP ili kompanija za e-trgovinu (eBay i PayPal su najpopularnije mete). Neke pecačke poruke očigledne su prijevare, ali druge su prava remek-djela, s logotipom kompanije i napisane jezikom korporativnog marketinga.

Pecačke poruke su općenito vrlo slične. U njima piše da postoji problem s vašim računom koji morate odmah riješiti te uključuju vezu do lokacije koja izgleda poput stvarne Web lokacije za prijavu odnosne kompanije. A lokacija je zapravo

lažna. Ona je identičan duplikat stvarne lokacije, ali se nalazi na poslužiteljima čiji su vlasnici kriminalci. U drugim slučajevima, veza može biti legitimna, ali kriminalci tako izmanipuliraju sustav adresiranja na Internetu da vas preusmjere na svoju lažnu lokaciju (što se ponekad naziva i "pharming").

Kliknete li na tu vezu, naći ćete se na stranici za prijavu koja je identična onoj s legitimne lokacije, s poljima za unos korisničkog imena, lozinke i broja računa. Mnoge *spoofirane* lokacije postaju pohlepne pa traže i druge informacije, poput vašeg matičnog broja. U želji da riješite probleme sa svojim računom vi – žrtva – marljivo upisujete sve tražene podatke. Ovisno o tome koliko su lukavi, kradljivci identiteta mogu vas i prebaciti na legitimnu lokaciju. Oni manje lukavi izdat će vam poruku o pogrešci. U međuvremenu, vaši se podaci prenose na poslužitelj koji kontroliraju kriminalci.

Kao da im ovo nije dovoljno "zločesto", pecači (*phisheri*) idu i dalje. Mnogi u poruke e-pošte uključuju zlonamjerne softverske programe. Ti programi mogu svašta. Neki bilježe pritiske na tipke na tipkovnici (*keystroke loggers*); a o njima govorimo poslije u ovom poglavlju. Drugi programi upućuju vaše računalo na *spoofirane* lokacije, čak i ako u Web pretraživač sami upišete Web adresu legitimne lokacije. Otkriven je jedan program koji ima popis bankarskih lokacija. Posjetite li jednu od lokacija s popisa, nakon što se prijavite, program automatski otvara nevidljivi pretraživač iza onog kojeg vidite na ekranu. Potom program provjerava stanje na vašem računu i prebacuje novac na račun pod nadzorom kriminalaca.

Još više zabrinjava rastuća vrsta napada u kojoj kriminalci oštete stvarnu stranicu za prijavu legitimne Web lokacije. To znači da u svoj pretraživač možete upisati www.vasabanka.com i nakon toga biti usmjereni na legitimnu Web lokaciju. Ali, kada upišete svoje podatke, zlonamjerni kod koji je prethodno umetnut na Web lokaciju hvata te podatke i šalje ih na računala u vlasništvu kriminalaca. Ovo je zastrašujuće otkriće, jer čak i ako sve dobro učinite, manjkavosti u izvedbi legitimne Web lokacije ostavljaju prostor za napad, a vi tu ništa ne možete učiniti.

Keystroke loggeri

Keystroke logger je program koji bilježi sve vaše pritiske na tipke tipkovnice. Te se informacije šalju udaljenom napadaču, koji skenira informacije da bi pronašao korisne dijelove podataka poput lozinki i brojeva računa. Neki *keystroke loggeri* dolaze s popisom Web lokacija poput bankovnih, kompanija za izdavanje kreditnih kartica i kompanija za e-trgovinu, te počnu bilježenje pritisaka na tipke kada u svoj pretraživač unesete URL s tog popisa. O *keystroke loggerima* detaljnije govorimo u 5. poglavlju "Kako se riješiti neželjenih gostiju?, 2. dio: *spyware, adware* i trojanski konji". Oni se prvenstveno koriste za krađe identiteta.

Krađa pošte i kopanje po smeću

Kradljivci identiteta mogu vam direktno iz poštanskog sandučića ukrasti ulaznu i izlaznu poštu. Razmislite samo koliko se informacija nalazi na izvodu za plaćanje računa po kreditnoj kartici: vaše ime, adresa, telefonski broj, broj kreditne kartice i broj računa za provjeru. Nabavite za dolaznu poštu poštanski sandučić koji se može zaključati, a odlaznu poštu bacajte u gradske poštanske sandučiće.

Svaki put kada poštom primate ili šaljete lozinke, kodove, PIN-ove i slične povjerljive podatke, nakon rada svakako ispraznite mape za poslane i primljene poruke, a njihov sadrLaj pospremite samo na zaštićeno mjesto. Koristite li Web-temeljenu adresu e-pošte, činite to neizostavno!

Manje sofisticirana, ali efikasna taktika naziva se kopanje po smeću *(dumpster diving)*. Ljudi u smeće bacaju razne vrste zanimljivih i potencijalno upotrebljivih informacija, poput izvoda iz banaka ili kompanija za izdavanje kreditnih kartica. Napadači mogu doći do tih informacija jednostavnim kopanjem po vašem smeću ili kontejnerima za recikliranje. Toliko o tome koliko se nisko tehnološki može ići a da se i dalje postižu rezultati. Najbolji način sprječavanja kopanja po smeću je uništavanje svih povjerljivih dokumenata prije njihova bacanja u smeće.

Kad smo već kod bacanja stvari, svakako moramo napomenuti da biste trebali izbrisati sadržaj svakog tvrdog diska kojeg ste naumili baciti. Jednostavno brisanje datoteka i formatiranje tvrdog diska nije dovoljno; postoje brojni softverski programi koji obnavljaju tako "izbrisane" informacije. Trebat će vam specijalan softver koji će vaš tvrdi disk pretvoriti u kaos nečitljivih podataka. Takvi alati su Web Eraser, WipeDrive i O&O SafeErase. Kompanija WindsorTech može izbrisati tvrdi disk preko Interneta. Posjetite adresu www.eraseyourharddrive.com.

2.2 Sprječavanje krađe identiteta

Postoji nekoliko načina za sprječavanje *online* krađe identiteta. Neki uključuju tehnologiju, ali se većina oslanja na zdrav razum. Počet ćemo sa zdravorazumskom prevencijom jer je efikasna i besplatna. Zatim ćemo prijeći na tehnološke opcije.

Razmislite prije nego što kliknete

Kao što smo već spomenuli, prijevaqre s namjerom krađe identiteta oslanjaju se na društveni inženjering i lažne poruke e-pošte. Najbolja obrana od tih vrsta napada je zdrav skepticizam za svaku poruku koja tvrdi da dolazi s neke lokacije za e-trgovinu ili iz financijske institucije. Sljedeći naputci mogu vam pomoći da izbjegnete "pecačke" napade temeljene na porukama e-pošte:

- Legitimne organizacije ne šalju poruke e-pošte u kojima od vas traže podatke o vašem računu.
- Korporacije budno paze da u korespondenciji s klijentima nema pravopisnih i gramatičkih pogrešaka. Pazite se poruka s pravopisnim i gramatičkim pogreškama i s čudnim frazama.
- Nemojte kliknuti ni na koju hipervezu u poruci. Pogledajte pažljivo te veze. One bi mogle imati čudne nastavke.
- Ako mislite da bi stvarno mogao postojati problem s vašim računom, najbolja opcija je da podignete telefonsku slušalicu i nazovete službu za korisnike. Ako to nije moguće, zatvorite poruku e-pošte i u svoj Web pretraživač sami upišite URL. Nikako nemojte izrezivati i uljepljivati URL iz poruke.
- Upotrijebite softver ili neki drugi alat, kao što je opisano poslije u ovom poglavlju, da biste provjerili je li lokacija *spoofirana.*
- Dobijete li poruku e-pošte iz banke ili s lokacije za e-trgovinu s kojima ne poslujete, izbrišite tu poruku bez otvaranja. Mnoge *phishing* poruke e-pošte sadrže viruse i drugi *malware* koji može zaraziti vaše računalo ako poruku otvorite.
- Koristite antivirusni softver, stalno ga ažurirajte i provjerite je li konfiguriran za automatsko skeniranje vaše e-pošte.
- Redovito provjeravajte svoje bankovne izvode i izvode kreditnih kartica. Trebali biste ispitati izvod od kreditne kartice ako je na njemu izviješteno neuobičajena aktivnost. Izvještaj o potrošnji po kreditnim karticama možete naručiti od svoje banke – pažljivo ga pregledajte.

Alati koji vam pomažu u sprječavanju krađe identiteta

Osim zdravog razuma i brojni vam alati mogu pomoći u sprječavanju krađe identiteta. Na vrhu popisa nalaze se antivirusni programi i *anti-spyware* programi. Budući da mnogo *phishing* poruka e-pošte sadrži viruse i zlonamjerni kod, svoj antivirusni softver morate stalno ažurirati. Također biste trebali investirati u *anti-spyware* softver (ili provjeriti obuhvaća li vaš antivirusni softver otkrivanje *spywarea*) i redovito skenirati svoje računalo. *Anti-spyware* softver može otkriti brojne vrste programa, poput *keystroke loggera* koje kradljivci identiteta koriste za dobivanje vaših osobnih podataka. O *spywareu* i *anti-spyware* rješenjima govorimo više u 5. poglavlju.

Također biste trebali poduzeti korake da svoj Web pretraživač zaštitite od programa s pokretanjem po učitavanju kojima zlonamjerne ili kompromitirane Web lokacije bez vašeg znanja instaliraju *malware* na vaše računalo. Zaštita putem Web pretraživača objašnjena je u 7. poglavlju "Zaštita Windowsa".

Drugi alati rade posebno s krađama identiteta i *phishingom.* U sljedeća poglavljima opisani su alati koji bi vas mogli zanimati. Neki od njih su besplatni, a druge ćete morati platiti.

SSL

Security Socket Layer (SSL) je protokol koji omogućuje šifrirani prijenos informacija putem HTTP-a (Hypertext Transfer Protocol, komunikacijski mehanizam za Web). SSL omogućuje korištenje digitalnih certifikata tako da Web pretraživač može provjeriti autentičnost neke Web lokacije. Digitalni certifikat oblik je elektroničke provjere vjerodostojnosti koji potvrđuje da je treća strana provjerila vjerodostojnost nositelja certifikata. Kada posjetite lokaciju svoje banke i prijavite se za provođenje neke transakcije, vaš Web pretraživač provjerava digitalni certifikat te lokacije da bi osigurao kako je www.onlinebanka.com zaista www.onlinebanka.com. Svi se Web pretraživači isporučuju s već učitanim sposobnostima za korištenje SSL-a – ništa ne trebate uključivati ili isključivati.

Postoje dva načina da provjerite koristi li se SSL. Adresa na traci za adrese Web pretraživača napisana je kao https:// a ne kao http://. (HTTPS je zaštićena verzija Hypertext Transfer Protocola.) Vidjet ćete i ikonu lokota u donjem desnom kutu pretraživača.

Međutim, imajte na umu da prisutnost ikone lokota ili https-a u pretraživaču ne može jamčiti da lokacija nije zlonamjerna. Kradljivci identiteta mogu registrirati lokaciju i koristiti SSL jednako lako kao i zakonske tvrtke. Premda biste trebali provoditi *online* transakcije samo na Web lokacijama koje koriste SSL, nisu sve Web lokacije koje ga koriste pravovaljane.

Isto tako, samo zato što legitimne tvrtke koriste SSL da bi zaštitile vaše podatke prilikom prijenosa, ne postoji jamstvo da će oni biti sigurno pohranjeni. Kao što smo napomenuli, lopovi stalno provaljuju u baze podataka korporacija da bi se domogli informacija. To vas ne mora nužno odbiti od e-trgovine, jer se brojevi kreditnih kartica koje koristite u materijalnom svijetu, u trgovinama, također nalaze u bazama podataka u koje se može provaliti. Problem nije u sigurnom prijenosu – problem je u sigurnom pohranjivanju i proceduralnoj zaštiti.

Sigurnosni tokeni

Kao što smo već napomenuli, jedan problem s e-trgovinom je taj da se sustav za provjeru autentičnosti oslanja na informacije poput korisničkog imena i lozinke koji se lako mogu pogoditi ili ih mogu ugrabiti *scameri*. Taj se problem može riješiti provjerom autentičnosti s dva faktora, koja kombinira nešto što znate (korisničko ime ili lozinka) s nečim što imate. Jedan od primjera provjere autentičnosti s dva faktora je sama bankovna kartica. Prvi faktor je PIN (nešto što znate). Drugi faktor je sama bankovna kartica (nešto što imate). Vaš je PIN beskoristan kriminalcima bez vaše kartice, kao što je ona neupotrebljiva bez PIN-a.

Provjera autentičnosti s dva faktora naročito je korisna za sprječavanje *online* krađe identiteta, jer čak i ako lopovi mogu ukrasti vaše korisničko ime i lozinku, on ili ona ne mogu ih upotrijebiti za korištenje vašeg računa bez posjedovanja drugog faktora.

U vrlo zaštićenim korporativnim ili vladinim postavkama, provjera autentičnosti s dva faktora provodi se jednim od trojeg: "pametnom" karticom (Smartcard, Activcard i sl.), biometrikom ili tokenom. Pametna kartica je komad plastike veličine kreditne kartice. On sadrži računalni čip u kojem je pohranjen digitalni certifikat koji na jedinstven način identificira vlasnika kartice, a pristupa mu se pomoću PIN-a. Biometrika je digitalizirana verzija fizičkih karakteristika poput otiska prsta ili skena rožnice ili zjenice oka. Token je mali uređaj koji generira nasumične brojeve u pravilnim intervalima; korisnik upiše broj zajedno sa svojim imenom za prijavu i lozinkom.

Kada govorimo o klijentima u e-trgovinama, tokeni su vjerojatno najviše zastupljena metoda provjere autentičnosti s dva faktora. Razlog tome je što pametne kartice i biometrika zahtijevaju posebne čitače koji se moraju instalirati na računalo korisnika. S vremenom će se sve više računala prodavati s ugrađenim ovim uređajima, ali sada su tokeni jednostavniji za primjenu jer ne zahtijevaju dodatni hardver na računalu.

Danas uobičajeni tokeni izgledom podsjećaju na male džepne kalkulatore s tipkovnicom za unos brojeva i ekranom – ali samo s jednom funkcijskom tipkom (dakle bez tipaka za zbrajanje, množenje i slično). Funkcionira tako da nakon unošenja inicijalne lozinke kombinira vaš PIN s brojem koji token sam generira složenom matematičkom pravilnošću i dobivenu vrijednost prikazuje na ekranu. Tom se kombinacijom znamenka predstavljate izdavaču tokena – najčešće banci. Svaki pojedinačni token ima vlastitu početnu vrijednost, pa dva tokena nikada ne mogu generirati isti broj.

Kada se korisnik želi prijaviti na lokaciju koja koristi provjeru autentičnosti s dva faktora, od njega će se tražiti da upiše višeznamenkasti broj zajedno s korisničkim imenom i lozinkom. Poslužitelj organizacije programiran je tako da zna početnu

vrijednost i vrijednost intervala za svaki token, pa može prepoznati ispravnost višeznamenkastog koda. Poslužitelj također zna koji je token dodijeljen pojedinom korisniku, tako da može korisnički ID pridružiti višeznamenkastom kodu koji token generira. I na kraju, poslužitelj prihvaća samo one višeznamenkaste brojeve koji se generiraju u određenom vremenskom okviru (primjerice, unutar posljednjih 5 minuta).

Da vidimo kako tokeni sprječavaju kradu identiteta. Recimo da lopov pošalje poruku e-pošte u kojoj od vas traži informacije za prijavu. Čak i ako korisnik pošalje te informacije, one su beskorisne bez koda tokena. Pa čak i ako korisnik pošalje napadaču svoju lozinku i broj koji je trenutačno prikazan na ekranu tokena, taj će broj vjerojatno biti beskoristan u vrijeme kada ga napadač pokuša upotrijebiti.

Gotovo svaka veća banka danas nudi mogućnost pristupa bankovnom računu pomoću tokena, tako da korisnici usluga banke mogu u bilo kojem trenutku rukovati novčanim sredstvima na vlastitom računu. Štoviše, tokenom je moguće osigurati pristup Internetu ili bilo kojim podacima do kojih pristup treba biti kvalitetno zaštićen; od podataka s burze i informacija koje su poslovna tajna pa do baze podataka lokalne knjižnice – no pristup podacima s tim stupnjem sigurnosti, odnosno pružanje takvih sigurnosnih usluga, u Hrvatskoj još nije prepoznato kao stvarna potreba.

Iako tokeni osiguravaju bolju zaštitu od jednostavne lozinke, i oni imaju svoje mane. Prvi je problem količina. Zamislite samo da su vam banka, ISP i e-trgovina s kojima poslujete dali tokene. Svaki put kada želite elektronički provesti transakciju, morat ćete kopati po ladici punoj tokena da pronađete ispravan. Tokeni s vremenom potroše svoje baterije, a mogu se izgubiti, ukrasti ili razbiti.

Još ozbiljniji problem je povećanje sofisticiranosti napadača. Provjera autentičnosti s dva faktora neće pomoći ako se na vašem računalu nalazi zlonamjerni program koji jednostavno čeka da se prijavite. A *scameri* mogu postaviti i lažnu Web lokaciju koja prosljeđuje vaše informacije (uključujući i kôd s tokena) na realnu lokaciju te se prijaviti u vaše ime. U oba slučaja učinak je isti: napadač će imati pristup vašem računu tijekom legitimne sesije i može provoditi transakcije. Kao što su stručnjaci za sigurnost u korporativnom svijetu otkrili, najbolja je strategija dubinske obrane, poput korištenja tokena uz dodatno održavanje računala sigurnim pomoću softvera za zaštitu.

SpoofStick

SpoofStick je mali program, takozvana ekstenzija pretraživača, koji vam može pomoći da otkrijete lažne Web lokacije. Program kreira novu alatnu traku u vašem pretraživaču koja prikazuje po kojoj Web lokaciji trenutno surfate. Na primjer, ako odete na www.ebay.com, alatna traka SpoofSticka ispisuje "You're

on ebay.com" (Nalazite se na ebay.com). Odete li na lokaciju koja se samo predstavlja kao eBay, SpoofStick izvještava samo IR adresu, a ne stvarno ime domene (na primjer, ispisuje "You're on 192.1.2.3."). Pokaže li SpoofStick IP adresu umjesto stvarnog imena domene, velike su šanse da lokacija po kojoj surfate nije pridružena organizaciji za koju se predstavlja.

Isti dan kada sam učitao SpoofStick, primio sam poruku e-pošte u kojoj je pisalo da svoj eBay račun moram ažurirati. Znao sam da je poruka prijevara, jer nemam eBay račun, ali sam kliknuo na vezu iz poruke da vidim hoće li SpoofStick otkriti lažnu Web lokaciju. I zaista jest. Iako su i lažna poruka e-pošte i *spoofirana* Web stranica bile vrhunske prijevare, to nije zavaralo SpoofStick. Alatna traka pretraživača ispisala je "You're on ..." s IP adresom. Nakon što sam izbrisao lažnu poruku, krenuo sam surfati po stvarnoj eBay lokaciji, i na svakoj stranici po kojoj sam *surfao* SpoofStick je marljivo izvještavao "You're on eBay.com."

SpoofStick je kreirao Phil Libin, predsjednik CoreStreeta, kompanije za sigurnost računala. Možete ga učitati za pretraživače Internet Explorer i Mozila Firefox na internetskoj adresi www.corestreet.com/spoofstick. Libin vodi i duhoviti *blog* koji se isplati posjetiti (www.vastlyimportant.com).

2.3 Oporavak od krađe identiteta

Unatoč najboljim mjerama predostrožnosti, i dalje je moguće da postanete žrtva krađe identiteta. (Zapamtite, čak i ako nikad ne otkrivate informacije o svojem računu, one se ipak mogu ukrasti iz baza podataka korporacija ili vlade, pa čak i iz vašeg novčanika ili torbice.) Prema Federalnoj trgovinskoj komisiji, gotovo je 10 milijuna ljudi bilo žrtvama krađe identiteta 2003. godine.

Oporavljanje od krađe identiteta zahtijeva strpljenje i upornost. Stručnjaci za oporavak od krađe identiteta preporučuju da dokumentirate sve svoje interakcije s raznim tvrtkama i agencijama s kojima radite, čuvate kopije svih zapisa, a svoje telefonske pozive kompanijama s kojima pokušavate riješiti krađu identiteta popratite i pismima. Evo i ostalih savjeta:

- Prijavite krađu banci, kompaniji za kreditne kartice ili davatelju usluga kod kojeg je otvoren lažni račun. Ako je netko u vaše ime otvorio novi račun, zatražite da ga zatvore. Zatražite razgovor s istražiteljem umjesto s predstavnikom službe za korisnike. Ako je netko zlorabio vaš postojeći račun, izvijestite o neautoriziranim terećenjima.
- Kontaktirajte glavne kreditne urede (American Express, MasterCard, Diners, Visa) da ih upozorite o prijevari. Kada pošaljete upozorenje jednom od tih

ureda, on će ih proslijediti ostalima. Upozorenje o prijevari sprječava otvaranje novih računa u vaše ime.

- Podnesite izvještaj lokalnoj policijskoj postaji. Banka ili kompanija za kreditne kartice mogle bi zatražiti policijski izvještaj prije nego što nastave rješavati krađe identiteta, pa zatražite kopiju izvještaja.
- Kontaktirajte Društvo za zaštitu potrošača i zatražite razgovor sa savjetnikom za zaštitu korisnika financijskih i bankarskih usluga – zakonske odredbe se često mijenjaju a one koje su na snazi ponekad se jednostavno ne primjenjuju – ako ste u nevolji trebate pomoć profesionalca koji je dobro upućen u trenutna zbivanja.

2.4 Popis za provjeru

Upotrijebite ovaj popis kao brzi referentni vodič za materijal iznesen u ovom poglavlju.

Učinite

- Zatražite kopiju svojeg godišnjeg kreditnog izvještaja. Možete poći na Web adresu svoje banke ili ih nazvati telefonom.
- Redovito provjeravajte bankovne izvode i izvode za svoje kreditne kartice ne biste li uočili znakove neobičnih ili sumnjivih aktivnosti.
- Budite sumnjičavi prema svakom neovjerenom kontaktu (telefonskom ili e-poštom) koji traži osjetljive informacije.
- Koristite antivirusni i *anti-spyware* softver da biste spriječili provaljivanje *malwarea* namijenjenog krađi identiteta u vaše računalo.
- Uništite povjerljive dokumente poput izvještaja od banaka i kompanija za kreditne kartice prije nego što ih bacite u smeće.
- Ako slutite da je vaš identitet ukraden ili imate dokaze da se to dogodilo, upozorite:
  - banke i tvrtke koje su vam izdale kreditne kartice
  - tvrtke s kojima poslujete.

Nemojte učiniti

- Nemojte odgovarati na poruke e-pošte u kojima se traže osobne identifikacijske informacije ili brojevi računa.
- Nemojte klikati na hiperveze u porukama e-pošte koje tvrde da dolaze iz neke banke ili kompanije za e-trgovinu.
- Nemojte uopće otvarati poruke e-pošte koje tvrde da dolaze iz banaka ili lokacija za e-trgovinu na kojima nemate račune.
- Nemojte otkrivati svoj jedinstveni matični broj kao identifikator, ako to nije nužno.

2.5 Korisni izvori

U Hrvatskoj zapravo i ne postoji volja državne uprave za prepoznavanjem kriminala koji proizlazi iz krađe identiteta, što je dijelom uvjetovano relativno malim brojem slučajeva i malom štetom. Policijske snage za informatički kriminal u Hrvatskoj još su zapravo u povojima. Želite li bolje razumjeti koji stupanj pozornosti možete očekivati od Ministarstva unutrašnjih poslova ako im se javte s problemom vezanim uz računalstvo, posjetite stranice www.mup.hr.

Ukoliko je riječ o međunarodnoj kriminalnoj aktivnosti, o većim se slučajevima izvještava Interpol.

Visa nudi savjete za zaštitu vašeg digitalnog identiteta i za sprječavanje toga da postanete žrtvama drugih oblika prijevara, poput telefonske. Posjetite adresu www.international.visa.com/ps/products/protect/main.jsp.

Nadalje iznosimo podatke koji vam mogu biti zanimljivi kao kuriozitet, jer prikazuju američku situaciju u vezi s problemom krađe identiteta.

Živite li kojim slučajem u Sjedinjenim Američkim Državama

Pokušaje *phishinga* možete prijaviti FTC-u na adresu e-pošte spam@uce.gov. Možete podnijeti i tužbu ako mislite da ste žrtva krađe identiteta. Pođite na adresu www.ftc.com i kliknite vezu File a Compliant na plavoj traci pri vrhu stranice. Da biste doznali više o drugim koracima koje možete poduzeti ako ste žrtva krađe identiteta posjetite stranicu www.conusmer.gov/idtheft koju također vodi FTC. I ona sadrži informacije o izvještavanju kreditnih agencija i zakonodavnih tijela o krađama. Možete nazvati FTC-ovu službu koja postoji zbog krađa identiteta na broj 877-IDTHEFT (877-438-4338) da biste dobili informacije i savjet.

Ako ste žrtva krađe identiteta, tužbu možete podnijeti i Centru za primanje tužbi u vezi kriminalnih djela na Internetu (Interet Crime Center – IC3, www.ic3.gov). ICT je udružena organizacija FBI-ja i Nation White Collar Crime Centera. Imajte na umu da podnošenje tužbe ne znači da će FBI preuzeti vaš slučaj. Vjerojatnije je da će se te informacije koristiti za istraživanje, ali će tužba možda biti proslijeđena lokalnom sudu za daljnju obradu. Vezu na obrazac za tužbu naći ćete na www.ic3.gov.

Identitiy Theft Resource Center je neprofitna grupa koja nudi informacije za pomoć klijentima da spriječe krađu identiteta ili se oporave od nje: www.idtheftcenter.org. Poput FTC-a ovaj centar ima korisne informacije o tome kako se oporaviti od krađe identiteta. Kliknite karticu Victim's Resources na lijevom dijelu stranice.

Anti-Phishing Working Group (APWG) je udruga tvrtki, davatelja usluga, proizvođača mehanizama za zaštitu računala i pravnih agencija. APWG prati *phishing* prijevare, održava arhivu *phishing* poruka e-pošte, razvija najbolje smjernice za tvrtke i potrošače da bi spriječili krađu identiteta i znali reagirati na nju te pruža obrazovne materijale. Sumnjate li na neku poruku e-pošte, provjerite *phishing* arhivu. Naći ćete je na adresi www.anit-phishing.org na vezi Phishing Archive na lijevoj strani početne stranice. *Phishing* poruke e-pošte možete i proslijediti toj grupi na adresu reportphishing@antiphishing.org.

Prisiljavanje tvrtki da prijave krađe identiteta

1. srpnja 2003. godine stupio je na snagu novi zakon poznat pod nazivom California Senate Bill (SB 1386). On primorava tvrtke s kalifornijskim klijentima da te klijente obavijeste o potvrđenim slučajevima neovlaštenog pristupa osobnim podacima ili o slutnji da se takav pristup dogodio. California Bill definira osobne informacije kao puno ime osobe (ili inicijal imena i prezime) u kombinaciji s jednim od sljedećeg:

- Jedinstveni matični broj
- Broj vozačke dozvole
- Broj računa, debitne ili kreditne kartice uz lozinku ili sigurnosni kod koji omogućuje pristup računu

Zakon također definira nekoliko vrsta obavijesti koje su prihvatljive:

- Pismena obavijest

- Elektronička obavijest
- Nadomjesna obavijest ako trošak obavijesti premašuje 250 000 američkih dolara ili ako treba obavijestiti više od 500 000 ljudi. Nadomjesna obavijest uključuje poruku e-poštom, vidno istaknutu obavijest na Web stranici organizacije ili objavu na nekom od medija.

Ovaj zakon također navodi da tvrtke nisu dužne prijaviti bilo kakvo kršenje osobnih informacija ako bi takve prijave utjecale na kriminalističku istragu koja je u tijeku.

Zakon je važan jer osigurava zakonsku prisilu da se zapravo počne izvještavati o kršenjima privatnosti, nešto što se inače ne bi dogodilo jer se korporacije općenito protive izvještavati o ozbiljnim provalama. Ovaj zakon također potiče tvrtke da se bolje brinu o vašim privatnim informacijama kako bi sebe poštedjele od neugodnosti, gubitka dobre volje klijenata i potencijalnih zakonskih tužbi koje bi proizlazile iz neovlaštenog otkrivanja informacija.

Ako ste jedan od milijuna Amerikanaca koji ne živi u Kaliforniji, mogli biste reći "Koga briga?". No, zakon se odnosi na tvrtke koje imaju klijente u Kaliforniji, a ne samo na tvrtke koje su locirane u Kaliforniji. Zato će i tvrtke izvan Kalifornije vrlo vjerojatno morati podnositi izvještaje o neovlaštenom otkrivanju osobnih podataka.

Jedan slučaj je incident ChoicePointa. U veljači 2005. godine, tvrtka za skupljanje podataka, koja čuva osobne podatke poput brojeva kreditnih kartica i matičnih brojeva milijuna potrošača, objavila je kako su scameri prijevarom tvrtku naveli da otkrije osobne podatke tisuća kalifornijaca. ChoicePoint, iako mu je sjedište u Georgiji, izdao je obavijest o slučaju zbog zakona SB 1386. Međutim, istražitelji su javno ispitivali jesu li lopovi ciljali samo stanovnike Kalifornije, a 19 je državnih javnih tužitelja zahtijevalo da sazna jesu li informacije o stanovnicima drugih država također kompromitirane. Pod pritiskom, ChoicePoint je priznala da su otkrivene i informacije stanovnika drugih država – više od 145 000 profila potrošača.

SB 1386 predložio je model za federalni zakon koji bi se primjenjivao na cijelu zemlju. Federalni prijedlog, koji je uvela kalifornijska senatorica Dianne Feinstein, poznat je kao Senate Bill odrednica, S.1350. Tekst predloženog zakona možete pročitati na adresi http://thomas.loc.gov/ home/search.html i potražiti članak S.1350 u 108th Congress.

Osobno iskustvo s potencijalnom krađom identiteta

U ožujku 2005. dobio sam pismo Boston Collegea, čiji sam bivši student. Za razliku od uobičajenih pisama bivšim studentima u kojima traže donacije, ovo je pismo opisivalo provalu u računalo koje sadrži osobne informacije – imena, adrese i telefone, te brojeve kreditnih kartica i matične brojeve – za otprilike 120.000 bivših studenata među kojima sam bio i ja.

Prema informacijama s koledža, uljez nije provalio da bi ukrao povjerljive informacije. Istraživanje BC-a je otkrilo da je napadač oteo računalo kao lansirnu rampu za napade na druge ciljeve.

Uz pismo u kojem sam obaviješten o provali, koledž je priložio popis činjenica s uputama za postavljanje upozorenja o prijevari preko Equifixa, Experiana i TransUniona, tri glavna kreditna ureda. Najprije sam pomislio da se neću gnjaviti s time, jer sam smatrao da je BC bio u pravu budući da se radi o napadaču čija namjera nije bila ukrasti podatke. No, nedavno nakon što sam završio pisanje ovog poglavlja o krađi identiteta, odlučio sam da to ipak ne bi bilo naodmet.

Nasumično sam odabrao Experian kao prvi ured. Cijelu se transakcija vodila preko automatiziranog sustava glasovnih uputa; ni u jednom trenutku nisam dobio opciju da govorim s čovjekom. Ali, ovim se sustavom jednostavno prolazi. Nakon zahtjeva za dodavanjem privremenog upozorenja o prijevari, koristio sam tipke na telefonu da bih upisao svoj matični i poštanski broj. Također sam odabrao i opciju da me kompanije za kreditne kartice nazovu da bi od mene dobile potvrdu prije otvaranja bilo kakvih novih računa u moje ime (za to sam trebao utipkati svoj telefonski broj). Tada mi je automatizirani sustav dao broj potvrde (tako da pri ruci morate imati olovku i papir, ako kroz ovo namjeravate proći). Experian mi je dao i opciju da podijelim ovo upozorenje s Equifixom i TransUnionom. Tu sam opciju prihvatio da bih sebe poštedio dva dodatna telefonska poziva i dodatnog utipkavanja. Nakon nekoliko dana primio sam pisma sva tri ureda koja su potvrđivala da je upozorenje o prijevari postavljeno na pravo mjesto.

Sljedeći poziv bio je da zatražim svoj kreditni izvještaj. Taj izvještaj možete tražiti od bilo kojeg kreditnog ureda. A možete i posjetiti specijalnu Web lokaciju da preko Interneta zatražite taj izvještaj. Ponovno sam morao

proći kroz automatizirani glasovni sustav. Ovaj je sustav malo kompliciraniji od Experianovog jer traži više informacija, uključujući adresu i datum rođenja. Sustav je pogrešno ispisao moju adresu, pa je malo potrajalo dok sam je ispravio. Ovaj sustav odgovara na tipke ili na glasovne naredbe, ali uz nekoliko pokušaja možete uspjeti.

Nakon toga sam kontaktirao ured za matične brojeve. No, predstavnik s kojim sam razgovarao rekao mi je kako administracija nema načina da mi kaže zlorabi li netko moj matični broj. Savjetovao mi je da poduzmem korake koje sam već opisao. Isto tako mi je rekao da bi, ako je moj matični broj zlorabljen, trebao dostaviti dokumentaciju u područni ured, koji će proučiti slučaj da provjeri treba li mi izdati novi matični broj.

Svoj posljednji poziv uputio sam lokalnoj stanici policije. Oko tog poziva sam se malo dvoumio, jer sam bio prilično siguran da ništa nije ukradeno, ali sam mislio da ne može štetiti. Upotrijebio sam običan broj (a ne 92), ali mi je odmah objašnjeno da krađa identiteta nije prioritet za policiju. S tog sam običnog broja preusmjeren na još jedan automatizirani glasovni sustav u kojem se ne nude nikakvi odabiri (provjera nečijeg statusa jamstva, izvještavanje o malodobnom kriminalu itd.). Nekako sam pronašao "put" do telefonske sekretarice patrolnog ureda za svoju mjesnu zajednicu. Ostavio sam poruku, ali nitko nije uzvratio poziv. (Ne krivim ih što me nisu nazvali; napokon, nikakav zločin nije počinjen koji možete vidjeti.)

Stručnjaci tvrde da je dobivanje policijskog izvještaja temelj za rješavanje slučajeva krađe identiteta, ali sam isto tako čuo da je to jedan od najteže ostvarivih zahtjeva jer lokalna policija jednostavno ne zna što učiniti s takvim zahtjevom. Moj je prijedlog, ako trebate ispuniti takav izvještaj, osobno otiđite u policijsku stanicu kako biste s nekim razgovarali (automatizirani telefonski sustav baš ne funkcionira). Na taj ćete način moći objasniti da vam je izvještaj nužan da biste zadovoljili zahtjev svoje banke ili kompanije za kreditne kartice, te možete uvjeriti službenika kako ne očekujete da će lokalna policija provesti istragu.

3. poglavlje

Vatrozidovi

Vatrozid (*firewall*) je softversko ili hardversko rješenje koje upravlja Internet komunikacijom prema vašem računalu ili od njega. On nadzire programe i aplikacije koji pokušavaju započeti komunikaciju s vašim računalom putem Interneta, te provjerava kojim je programima na vašem računalu dopušteno da prenose informacije na Internet.

Vaša vam je majka rekla: "Nikad ne razgovaraj sa strancima!", i to iz dobrog razloga – mnogo je ljudi kojima ne možete vjerovati. Taj savjet vrijedi i za Internet. Ispravno konfiguriran vatrozid je u osnovi kompjutorizirana verzija uputa vaše majke. Internet vrvi računalima kojima ne možete vjerovati, a vatrozid vas može zaštititi od uplitanja vašeg računala u konverzaciju sa strancima. Drugim riječima, on može spriječiti nepoželjne veze s računalima na Internetu. To je odvojeno od poželjnih veza poput one kada pokrenete svoj Web pretraživač i u polje za adresu upišete određeni URL ili kada provjeravate svoju e-poštu. Tada uspostavljate vezu s drugim računalom, a to računalo potom sudjeluje u razmjeni informacija. Primarna uloga vatrozida je upozoravati vas na pokušaje uspostavljanja nepoželjnih veza koje potom blokira.

Vatrozidovi su dobra zaštita protiv raznih vrsta opasnosti, kao što su napadači koji skeniraju Internet u potrazi za potencijalnim žrtvama i automatizirani crvi. Kao što ste naučili iz 1. poglavlja "Opasnosti koje prijete na Internetu", crvi su programi koji mogu pokušati iskoristiti 'pukotine' u softveru da bi dobili pristup

i kontrolu nad što je moguće više računala. Vatrozidovi su efikasni pri otkrivanju nekih vrsta crva koji se oslanjaju na nepoželjne veze, u kojima računalo koje niste kontaktirali pokušava pristupiti vašem računalu.

U tekstu koji slijedi opisat ćemo načine na koje vaše računalo komunicira s drugim računalima na Internetu. Tako ćete dobiti bolji uvid u to kako vatrozid radi što već radi, i zbog čega je on vrijedan alat za svakoga tko koristi Internet. Sljedeća poglavlja redom opisuju dva vatrozida koja možete besplatno nabaviti, te objašnjavaju razloge zbog kojih se isplati platiti softversku zaštitu. Ovo je poglavlje posvećeno isključivo softverskim vatrozidovima (odnosno vatrozidovima koje instalirate na svoj tvrdi disk kao i bilo koju drugu softversku aplikaciju). Hardverski vatrozidovi imaju istu funkciju ali se nalaze na posebnom uređaju koji se nalazi između vašeg računala i veze s Internetom. Mnogi korisnički usmjernici (*routeri*) koji omogućuju da više računala dijeli pristup Internetu sadrže i vatrozid.

3.1 Paketi, protokoli i portovi

Što više učim o Internetu to sam više očaran činjenicom da on stvarno funkcionira. Mnogi su briljantni umovi naporno radili da bi sakrili organičku složenost Interneta iza prijaznih sučelja aplikacija. Ovaj odjeljak guli jedan ili dva sloja tog "pokrova" kako bi vam pomogao da više cijenite način na koji Internet funkcionira i razumijete zašto su kontrole poput vatrozida neophodne. Ako vas nimalo ne zanima kako Internet funkcionira, možete preskočiti sljedeći odjeljk. No, pročitate li ga, u najmanju ćete ruku moći impresionirati svoje "neuke" prijatelje raspravljanjem o tehnološkim osnovama Interneta.

Osnovna jedinica Internet komunikacije naziva se paket. Svaka Web stranica koju vidite, poruka e-pošte koju primite ili datoteka koju preuzimate najprije se dijeli na male pakete, od kojih se svaki pojedinačno isporučuje na vaše računalo. Ono zatim ponovno sastavlja te paketiće u suvislu cjelinu koju vam prikazuje.

Načinima na koje se paketići konstruiraju, adresiraju i usmjeravaju preko Interneta rukovodi skup pravila koja osiguravaju zajednički radni okvir koji svako računalo slijedi. Ta se pravila nazivaju protokoli. Protokole nadziru razna vodeća tijela poput Internet Engineering Task Force (IETF, www.ietf.org) i Institute of Electrical and Electronics Engineers (IEEE, www.ieee.org).

Svaki protokol ili aplikacija koristi portove za spajanje na pojedinačna računala. Portovi su pristupna vrata kroz koja informacije dolaze u računalo i odlaze od njega. Danas je u upotrebi 65 535 mogućih portova, a neke aplikacije koriste

posebne portove. Na primjer, HTTP (Web) promet koristi portove 80 i 8080, a HTTPS (šifrirani Web promet) koristi port 433. Programi za dijeljenje datoteka i sustavi za dopisivanje u realnom vremenu koriste razne portove; mnogi od tih programa imaju upute da koriste bilo koji raspoloživi port.

Budući da aplikacije koriste portove za pristup računalima, jedan od poslova vatrozida je da nadzire koji portovi smiju komunicirati s računalom. Portovi su logički, a ne fizički, pa se nemojte zamarati traženjem 65 535 sićušnih vrata na stražnjoj strani svojeg računala.

IP i TCP

Kamen temeljac protokola za Internet jesu IP (*Internet Protocol*) i TCP (*Transmission Internet Protocol*). Možda ste čuli za IP vezano uz *Voice over IP* (VoIP), novu tehnologiju koja omogućuje telefonske pozive putem Interneta.

IP opisuje način na koji se šalju paketi s jednog na drugo računalo. Svako računalo na Internetu ima neku adresu (IP adresu). Ta se adresa sastoji od četiri grupe s do tri broja, od kojih je svaka odijeljena zarezom ili točkom. Evo primjera jedne IP adrese: 192.101.432.156.

Ako za pristup Internetu koristite *dial-up* modem vaš davatelj usluge vašem računalu dodjeljuje novu IP adresu svaki put kada pristupate Internetu. Ista se stvar događa s kabelskim modemima i DSL (*Digital Subscriber Line*) vezama, osim što IP adresa ostaje s vama tako dugo dok se ne odjavite s veze ili isključite računalo. Mnogo ljudi koji koriste kabelske modeme ili DSL veze Internet ostavljaju uključenim danima ili tjednima.

Iako je praktično imati trenutačan pristup Internetu, dugotrajne IP adrese mogu postati rizične.

To je zbog toga što kriminalci stalno skeniraju Internet koristeći se posebnim softverskim alatima u potrazi za strojevima u koje je lako provaliti. Skeniranje širokih područja na Internetu traje, a ti alati uočavaju potencijalno ranjive IP adrese na koje se provalnik može poslije vratiti. Ako je vaša IP adresa trajna, tada će provalniku biti jednostavno ponovno vas pronaći. Na primjer, kreator crva Blaster.B koristio je prije zaražene strojeve kao stanice za izdavanje naredbi za pokretanje još više napada. On je znao da su te stanice raspoložive i tjednima nakon što je u njih provaljeno jer su bili spojeni na kabelske modeme, pa se IP adresa nije mijenjala. (Veze velike brzine također su vrlo popularne među Internet kriminalcima jer preko njih mogu mnogo brže pokrenuti napade nego preko *dial-up* veza.)

Svaki bi Internet korisnik trebao imati vatrozid jer svaki Internet korisnik ima neku adresu – a vatrozid je poput postavljanja brave na vrata. Trenutačno je Internet pun nezaključanih vrata, a kriminalci imaju svoje mete. Korištenjem ispravno konfiguriranog vatrozida izlazite iz gomile lakih meta. Ovo ilustrira nešto važno o sigurnosti računala; vaš sigurnosni sustav ne mora biti savršen – on samo mora biti bolji od onog vaših susjeda. Ako po noći zaključavate vrata, a vaši susjedi svoja ostavljaju otključana, mudri će kriminalci provaliti tamo gdje je to jednostavnije učiniti.

Kao što smo napomenuli, kada jedno računalo šalje informacije drugom računalu, ono te informacije dijeli u pakete. Svaki je paket markiran IP adresom računala pošiljatelja (adresa izvora) i IP adresom primatelja (adresa odredišta). Svaki paket sadrži i dio cjelovite informacije koja se šalje na odredište (taj se dio informacija naziva *payload*). Pošiljatelj šalje svoje pakete preko lokalnog usmjernika. Usmjernik (*router*) je računalo u mreži čiji je posao da prosljeđuje pakete s jednog na drugo mjesto. Usmjernici održavaju zapise koji se nazivaju tablice, a u kojima su opisani najbolji putovi do raznih odredišta na mreži. Paketi mogu putovati kroz brojne usmjernike prije nego što stignu na računalo-primatelj.

IP je poznat kao protokol "najboljeg pokušaja". Taj protokol nema mehanizam za provjeravanje jesu li paketi stigli na svoje odredište. On jednostavno "istresa" pakete na mrežu i nada se da će oni dospjeti na odredište.

Da bi se dodalo više kontrole slanju i primanju poruka, razvijen je TCP protokol. TCP prijenosu dodaje niz brojeva tako da računalo-primatelj zna koliko paketa očekivati (na primjer, ovo je paket broj 5 od osam paketa). TCP također pruža mehanizme za osiguravanje dospijeća svih paketa, a ako to iz nekog razloga ne uspije, tada se ponovno šalju paketi koji nedostaju. Na temelju usmjerničkih odluka tijekom putovanja, paket broj 5 može stići prije paketa broj 4. Računalo-primatelj čuva pakete dok svi ne stignu a zatim ih ponovno sastavlja prema ispravnom redoslijedu i prosljeđuje drugim slojevima računala na obradu.

TCP je poznat kao protokol stanja jer on nadzire stanje prijenosa. Umjesto "istresanja" paketa na Internet, TCP kontaktira računalo-primatelj i nadzire prijenos kako bi osigurao da svi paketi stignu na odredište. Ako se to ne dogodi, računalo-primatelj može zahtijevati ponovno slanje paketa koji nedostaju.

HTTP i HTML

Ova grupa protokola tehnički ne predstavlja Internet protokole. To su protokoli World Wide Weba. Iako mnogo ljudi govori o Internetu i Webu kao o istoj stvari,

oni su zapravo zasebni entiteti. U čemu je razlika? Internet je mehanizam povezivanja fizički udaljenih računala. World Wide Web je formalizirani način predstavljanja informacija i navigiranja kroz repozitorije informacija (poput Web lokacija). Web isto tako "jaše" povrh Interneta; odnosno protokoli koje koristi Web prenose se protokolima, uključujući IP i TCP s mjesta na mjesto.

Tim Berners-Lee, britanski fizičar, izumio je World Wide Web kreirajući Hypertext Markup Language (HTML) i Hypertext Transport Protocol (HTTP). HTML je jezik za kreiranje Web stranica. HTTP je mehanizam za prijenos HTML-a.

HTML upućuje Web pretraživače kako predstaviti tekst i daje korisnicima sposobnost klikanja na veze umetnute u tekst. Izvorni HTML kod možete vidjeti na Web stranici u pretraživaču Internet Explorer otvaranjem izbornika View na vrhu stranice i odabirom stavke Source.

Berners-Leeov najznačajniji doprinos je to što je umjesto patentiranja svoje ideje, tu ideju učinio besplatno dostupnom svakome tko bi je poželio. To je dovelo do procvata kreativnosti koja je Web učinila tako široko rasprostranjenim medijem prepunim informacija.

Drugi kamen temeljac u razvoju World Wide Weba je kreiranje Web pretraživača Netscape Navigatora. Autora Marca Andreessena i Jima Clarka, pretraživač Netscape stvorio je uobičajeno okruženje za pregledavanje Web stranica. Današnji su Web pretraživači postali najkorišteniji mehanizmi preko kojih ljudi istražuju World Wide Web i Internet.

3.2 Što vatrozidovi mogu učiniti?

Ovo smo poglavlje započeli usporedbom vatrozidova i majčinskog savjeta da ne razgovarate sa strancima. Sada ćemo više govoriti o tome kako vas vatrozidovi mogu zaštititi i istražiti njihova ograničenja.

Regulirajte ulazne i izlazne veze

Primarna funkcija vatrozida je regulirati ulazne i izlazne veze vašeg računala. On to radi tako da istražuje svaku aplikaciju ili protokol koji pokušava otvoriti neki port na vašem računalu. Toga možda i niste svjesni, ali kada ste na Internetu, programi stalno kucaju na vaša vrata. Ako imate instaliran vatrozid, možete njegove postavke odrediti tako da vas upozorava svaki put kada neki program pokuša uspostaviti vezu s vašim računalom. Često se radi o programima za

skeniranje portova, a to su softverski alati koji skeniraju ciljne strojeve u potrazi za otvorenim portovima koje mogu upotrijebiti da bi pristupili vašem računalu.

Za vatrozid je također važno da može zaustaviti vaše računalo u "razgovoru" s Internetom. Ako na svojem računalu imate trojanske konje, *spyware* ili druge vrste *malwarea*, vatrozid ih može spriječiti pri uspostavljanju izlazne veze s drugim računalima. Ovo je nužno jer se na taj način sprječava da vaše računalo postane izvor napada na druga računala, da *spyware* izvještava o vašim aktivnostima ili da *malware* komunikacijom s kontrolnim sustavom pribavi nove naredbe ili se ažurira.

Dobar vatrozid trebao bi moći sljedeće:

- Učiniti vaš PC nevidljivim. Zapamtite da vaše računalo ima 65 535 portova, a svi se mogu upotrijebiti za uspostavljanje veze s drugim računalom na Internetu. Iako je važno da računalu dopustite korištenje portova pridruženih popularnim aplikacijama poput Weba, e-pošte i sustavu razmjene poruka u realnom vremenu, ne postoji razlog zbog kojeg bi nepoznata računala na Internetu trebala pokušavati pristupiti vašem stroju putem neuobičajenih portova. Jedan od načina na koji kriminalci s Interneta provaljuju u računala je pokušavanjem otvaranja veza na svakom mogućem portu ciljanog sustava. To rade tako da šalju TCP-IP zahtjeve; ako se ciljno računalo odazove na određeni zahtjev, napadač je pronašao potencijalni ulaz u vaše računalo.

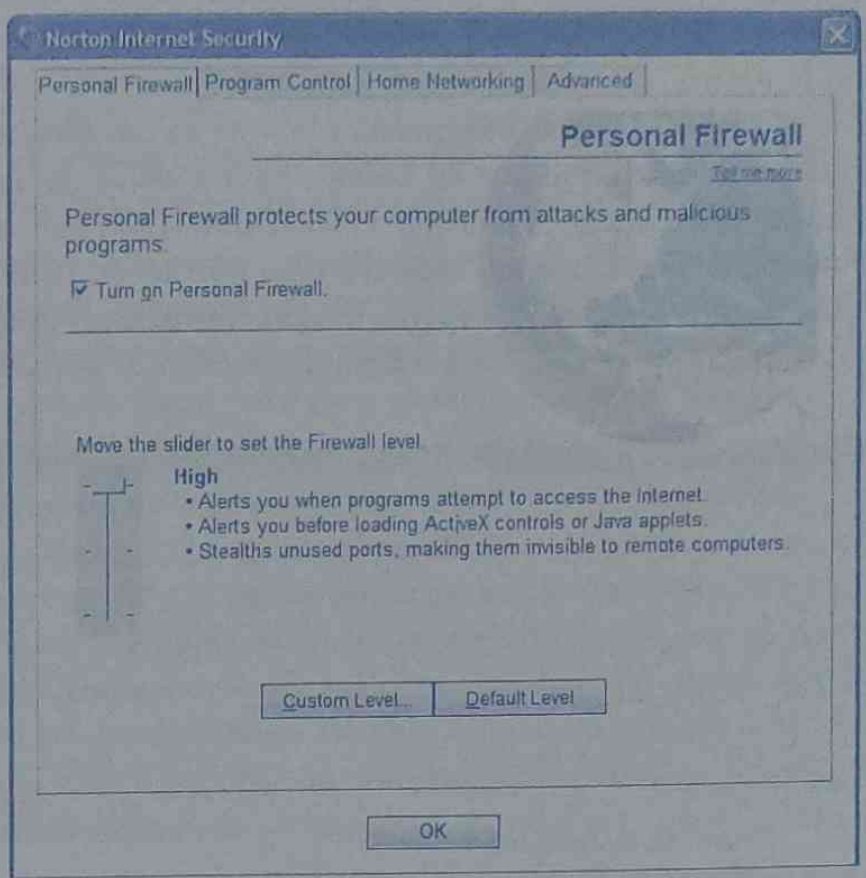
  Zato, dobri vatrozidovi ne odgovaraju na TCP/IP zahtjeve portovima koji se ne upotrebljavaju za uobičajeno korištenje Interneta. Neodazivanjem vaše računalo postaje nevidljivo. Ovo se često naziva stavljanje računala u prikriveni način rada (*stealth mode*).
- Upozoriti vas na sumnjivo ponašanje. Vatrozid bi trebao biti u stanju reći vam kada neki program ili veza pokušava učiniti nešto nepoželjno, poput kopiranja softvera na vaše računalo ili pokretanja programa kao što je ActiveX. (ActiveX je Microsoftova tehnologija koja izvršava programe učitane iz Internet Explorera. Neki su ActiveX programi benigni, ali napadači ih mogu koristiti za umetanje *malwarea* na računalo korisnika. Detalje o ActiveX programima naći ćete u 5. poglavlju "Kako se riješiti nepozvanih gostiju?, 2. dio: *spyware*, *adware* i trojanski konji".) No, ova značajka ima i svoje mane. Lako je potvrdno odgovoriti nazahtjeve za vezama s pouzdanih Web lokacija, ali mnoge poruke upozorenja teško je razumjeti. Neki vatrozidovi kao što je Zone Alarm Pro, mogu pružati dodatne informacije

o upozorenjima da vam pomognu u odlučivanju trebate li neku akciju ili vezu dopustiti.

- Blokirati izlazne veze koje niste pokrenuli. Kao što već rekosmo, *malware* na vašem računalu može pokušati kontaktirati druge strojeve na Internetu. Niste li izravno pokrenuli neki program, dobar će vas vatrozid obavijestiti kada program s vašeg računala pokušava na svoju ruku pristupiti Internetu.

Postavke sigurnosti

Većina vatrozidova omogućuje vam da podesite postavke sigurnosti. Na primjer, Norton Internet Security uključuje kliznu traku koja ima razine Low, Medium i High (niska, srednja i visoka), kao što se vidi na slici 3.1. Ove postavke podešavaju razinu zaštite koju vatrozid pruža. Općenito govoreći, što je postavka viša, veća je zaštita.



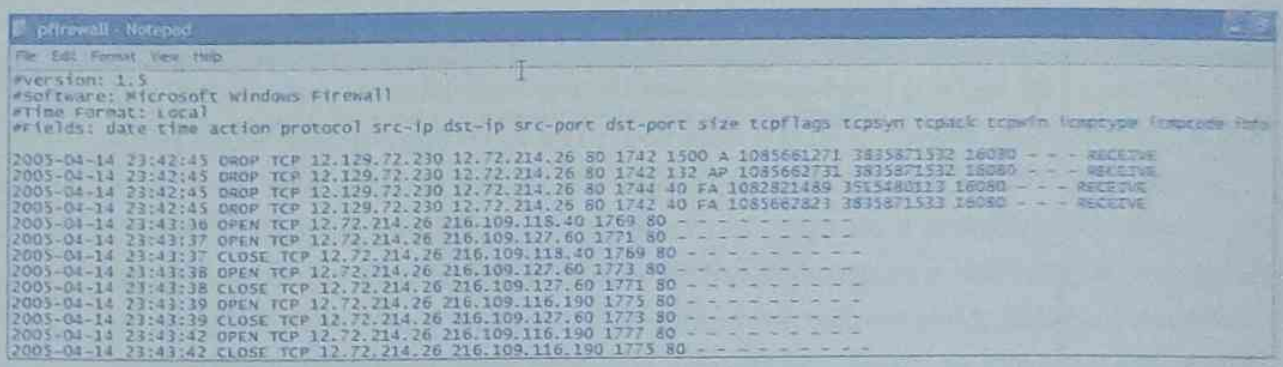
Slika 3.1 Postavke Norton Internet Security

Međutim, više postavke načelno mogu smetati pri korištenju Interneta. Preoprezni vatrozidovi mogu prekidati *surfanje* Webom, preuzimanje datoteka i druge procese koje smatrate normalnim, ali im vatrozid ne vjeruje. U krajnjem slučaju mogli biste provesti mnogo vremena klikajući gumb Allow da bi se nastavio prekinuti postupak.

Jedan od načina da saznate koja je razina zaštite za vas najbolja je da počnete s najvišom postavkom pa vidite koliko smetnji ona uzrokuje. Tada možete postupno snižavati razinu dok ne dosegnete onu koja vam najbolje odgovara. Imajte na umu ono što gubite i ono što dobivate: niža sigurnost općenito poboljšava jednostavnost korištenja ali i povećava izloženost napadima i infiltriranju. Trebat ćete pronaći odgovarajuću ravnotežu.

Napredni korisnici će možda htjeti "prčkati po utrobi" vatrozida, igrajući se s pravilima koja uključuju više koraka od jednostavnog pomicanja klizača s High na Low, kao što je blokiranje određenih portova ili aplikacija.

Vaš vatrozid bilježi i sve strojeve s kojima komunicira. Taj se popis naziva dnevnik vatrozida (*firewall log*). On vam neće izgledati baš smisleno ako nemate iskustva s računalnim mrežama. No, želite li vidjeti kako izgleda neka IP adresa, koje portove koristi vaše računalo i IP adrese mjesta s kojima se povezujete, tada biste taj dnevnik mogli pregledati. Windows XP Service Pack 2 uključuje ugrađen vatrozid. Zadano odredište za datoteke dnevnika je C:WINDOWS/pfirewall, kao što se vidi na slici 3.2, ali ta datoteka može biti zapisana gdje god želite. Zamijetite da ova funkcija bilježenja radi samo za Windows Firewall. Vatrozidovi drugih proizvođača kreiraju vlastite dnevnike koje biste trebali pronaći preko korisničkog sučelja.



Slika 3.2 Dnevnik vatrozida

Format dnevnika uključuje datum i vrijeme svake akcije, opis akcije (na primjer, otvaranje veze s drugim računalom), protokol (TCP itd.), IP adrese izvora i

odredišta, portove izvora i odredišta te informacije o individualnim paketima koji čine Internet komunikaciju.

3.3 Što vatrozidovi ne mogu učiniti?

Vatrozidovi su važna komponenta kućne sigurnosti, ali i oni imaju svoje granice. Mnogi napadi s Interneta koriste portove i aplikacije kojima se obično dopušta da prolaze kroz vatrozid, uključujući Web i e-poštu. Stoga, ako vaš vatrozid dopušta Web i promet e-pošte (a ako ne dopušta onda niti nema smisla išta počinjati s Internetom), vatrozid vjerojatno neće spriječiti napade koji koriste te ulaze.

Na primjer, najpopularniji način inficiranja virusima i crvima je prilog poruci e-pošte (*attachment*). Tako dugo dok je vaš vatrozid konfiguriran za dopuštanje prometa poruka e-pošte, on je nemoćan u zaustavljanju virusa koji dolaze kao prilozi u porukama e-pošte.

To na neki način isto vrijedi i za Web. Mnoge Web stranice koriste razne softverske programe kao što su kolačići, ActiveX i Java da bi ubrzali pretraživanje i učinili ga vizualno zanimljivijim. Međutim, te programe napadači mogu zlorabiti tako da na Web stranice umetnu *malware*. *Malware* se kopira na vaše računalo kada *surfate* po toj Web lokaciji (to se ponekad naziva 'pokretanje po učitavanju').

Na kraju, vatrozidovi rade samo ono što im naredite. Ako vas vatrozid pita želite li određenom programu dopustiti izvođenje a vi potvrdno odgovorite, pa ako taj program ispadne zlonamjeran, ne možete kriviti vatrozid. Odlučivanje o tome dopustiti ili ne uspostavljanje neke veze vjerojatno je jedan od najtežih dijelova zaštite računala za kućne korisnike.

Postoji nekoliko načina na koje se možete nositi s upozorenjima koja ne razumijete. Nalazite li se na lokaciji s dobrom reputacijom, kao što su dobro poznate lokacije za e-trgovinu, ISP-i ili bankarske lokacije, vjerojatno možete bezbrižno dopustiti izvršavanje programa. Na primjer, kada god nekoj poruci e-pošte pridružim datoteku koristeći Yahoo! Mail, moj me vatrozid upozorava da se neki ActiveX program želi izvršiti. Uvijek kliknem Allow jer vjerujem u Yahoo!. Ako želite biti oprezniji, druga je opcija da odbijete akciju. No tada postoji opasnost da aplikacija ili transakcija neće funkcionirati, pa ćete sve morati početi iznova.

Druga opcija je kopiranje imena programa, aplikacije ili usluge koja pokušava uspostaviti vezu i ulijepiti ga u polje za pretraživanje vaše omiljene tražilice. Rezultati koje dobijete mogu vam pomoći da odlučite možete li dopustiti uspostavljanje veze.

Za potpuniju zaštitu, softver vatrozida trebao bi se koristiti u sprezi s antivirusnim i *anti-spyware* softverom, o kojima također govorimo u ovoj knjizi.

3.4 Besplatni vatrozidovi

Skroman budžet nije izgovor za lošu zaštitu računala. Ovaj odjeljak opisuje dva vatrozida koja možete preuzeti s Interneta besplatno. Iako su ova dva vatrozida najpoznatija, u tablici 3.2 nalazi se popis preostala tri besplatna vatrozida.

Windows XP Service Pack 2

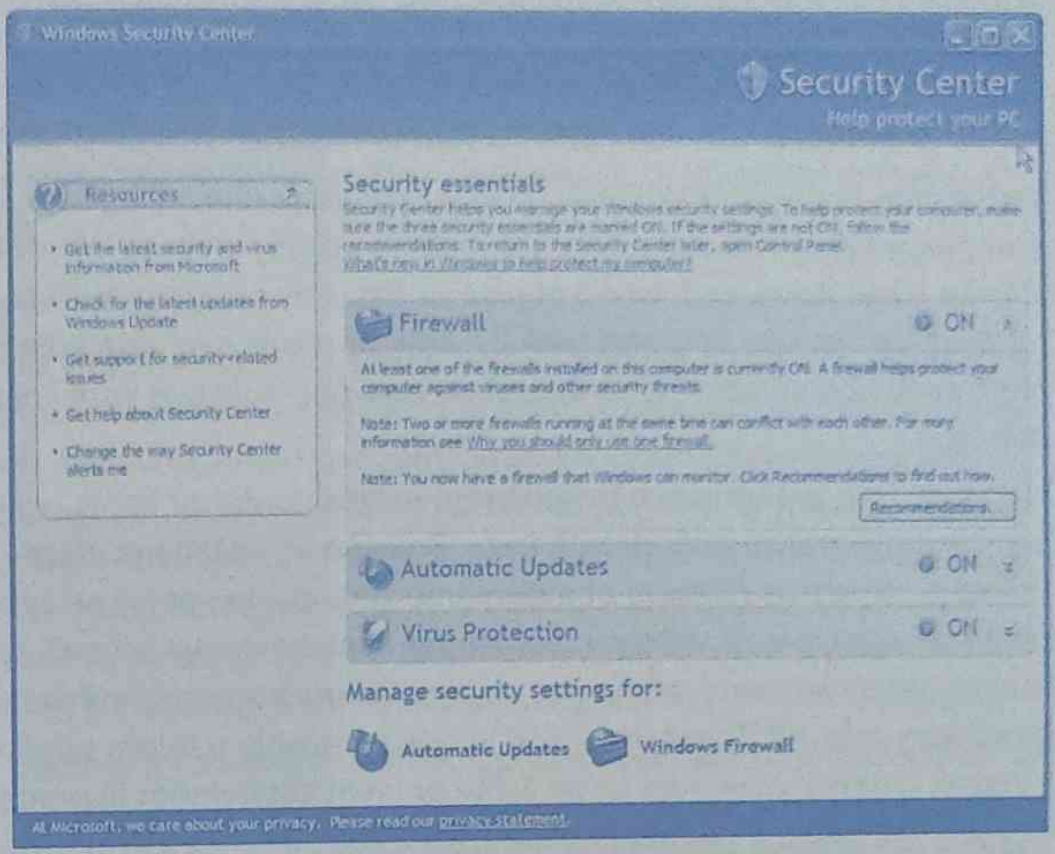
Korporacija Microsoft kažnjena je vlastitim uspjehom. Budući da se radi o najrasprostranjenijem operativnom sustavu za PC-e na svijetu, on je isto operativni sustav koji najviše ciljaju napadači s Interneta. Pisci *malwarea* i zli hakeri rutinski otkrivaju nove 'rupe' u operativnom sustavu Windows i drugim aplikacijama Microsofta i koriste ih za otimanje PC-a, krađu ili oštećivanje podataka i druge kriminalne radnje putem Interneta.

Najpoznatiji su virusi i crvi u posljednjih nekoliko godina (Blaster, Slammer, MyDoom, Code Red, Nimda itd.) svi ciljali Windowse, Internet Explorer i ostale Microsoftove aplikacije. Dok neki ljudi tvrde da je svaki publicitet dobar, ponavljano iskorištavanje Microsoftovih proizvoda natovario je kompaniji kritike pa su mnogi korporativni klijenti počeli razmatrati alternativna rješenja poput Linuxa. (Korisnici računala bi trebali ozbiljno razmisliti o prelasku na Macove, koji imaju mnogo manje problema sa sigurnošću. Naravno, postanu li Macovi toliko popularni koliko su to Windows PC-i mogu vam jamčiti da će kriminalci s Interneta brzo pronaći način na koji ih mogu koristiti. Za sada je, međutim, Mac platforma najsigurniji izbor za korisnike.)

Microsoft se odazvao nastojeći napisati znatno sigurniji kôd i uključiti sigurnosne značajke u svoje proizvode. Sa strane korisnika, njegov je najveći korak prema sigurnijem računalnom okruženju Windows XP Service Pack 2 (SP2), najnovija nadogradnja Microsoftovog operativnog sustava. SP2 nadogradnja besplatno je dostupna (uz pretpostavku da ste kupili XP – oni na čijim se računalima izvode Windows 98, Windows 2000, Windows Me, ili, neka vam Bog pomogne, Windows 95 nemaju tu sreću).

SP2 možete preuzeti s Windows Update (ali se radi o velikoj datoteci, pa odvojite dovoljno vremena, osobito ako koristite *dial-up* vezu). Sve potrebne podatke o SP2 potražite na adresi www.microsoft.com/windowsxp/sp2/default.mspx ili na www.microsoft.com/croatia (upišite samo www.microsoft.hr).

SP2 obuhvaća Windows Security Center, prikazan na slici 3.3, koji nadzire osnovne informacije sigurnosti o vašem računalu. On koristi jednostavne ikone štitova u zelenoj, žutoj i crvenoj boji da označi status sigurnosti vašeg računala. Nakon instaliranja softvera, Security Center možete naći tako da otvorite Control Panel. Security Center omogućuje vam da kontrolirate tri sigurnosne značajke SP2: Windows Firewall, Automatic Updates i Virus Protection.



Slika 3.3 Windows Security Center

Windows Firewall

SP2 uključuje besplatni softver vatrozida dizajniran posebno za Windows XP. On blokira pokušaje uspostavljanja nepoželjnih ulaznih veza koje poduzimaju računala ili programi na Internetu. Crvi, virusi i provalnici pokušavaju se spojiti koristeći se raznim portovima i protokolima. Windows Firewall može blokirati pokušaje povezivanja. No, kao i s drugim vatrozidovima, morate zadati Windows Firewallu

koje veze želite dopustiti, a koje blokirati. Kada kliknete Yes da dopustite uspostavljanje neke veze, kreirate izuzetke pravilima vatrozida; kada jednom kreirate izuzetak, vatrozid neće ubuduće blokirati program s popisa izuzetaka.

Neki programi zahtijevaju izuzetke da bi ispravno funkcionirali; na primjer, sustav za slanje i primanje poruka u realnom vremenu, dijeljenje datoteka i *online* kockanje često koriste razne portove. Međutim, što više izuzetaka kreirate, to više portova ostavljate otvorenim. Kao što je već napomenuto, kriminalci s Interneta stalno skeniraju Internet u potrazi za otvorenim portovima koji će im omogućiti povezivanje s vašim strojem. Zato je u vašem interesu da ograničite broj izuzetaka koje kreirate.

Windows Firewall također sadrži dnevnik. Taj dnevnik bilježi aktivnost vatrozida, te blokirane i dopuštene veze. Ne trebate trošiti vrijeme na proučavanje tih dnevnika, ali vam oni mogu pružiti korisne tragove ako vidite da se određeni programi čudno ponašaju ili ako sumnjate da vam je računalo zaraženo *malwareom.*

Trebat ćete eksplicitno aktivirati funkciju kreiranja dnevnika jer ona prema osnovnim postavkama nije aktivirana. Da biste to učinili, otvorite Windows Firewall i kliknite jahač Advanced. Ispod popisa za Security Logging možete odabrati jednu od dvije opcije: Log dropped packets, koja popisuje sve veze koje je vatrozid blokirao ili Log successful connections, koja popisuje sve veze koje je vatrozid dopustio.

Naravno, iako je zamisao o besplatnom vatrozidu dobar korak, vatrozid SP2 štiti samo od neautoriziranih ulaznih veza. Premda su neželjene ulazne veze najveća prijetnja, Windows Firewall obavlja samo pola posla, jer on ne zaustavlja postojeći *malware* na vašem računalu od uspostavljanja izlaznih veza. Zato ćete možda htjeti razmotriti ostale alternative. Većina komercijalnih vatrozidova (i besplatan vatrozid ZoneAlarm, koji je opisan poslije u ovom poglavlju) nadzire i ulazne i izlazne veze. Ako se ne želite gnjaviti kupovinom ili preuzimanjem drugog vatrozida, u najmanju biste ruku trebali iskoristiti Windows Firewall.

Ako imate instaliran i neki drugi vatrozid, ili ako želite koristiti neki drugi vatrozid, nemojte misliti da ćete biti dvostruko zaštićeni ako koristite vatrozid drugog proizvođača istodobno s Windows Firewallom. Zapravo, istodobno izvođenje dvaju ili više vatrozidova na istom računalu može vam smetati pri korištenju Interneta. Da biste onemogućili Internet vatrozid, kliknite ikonu Windows Firewall na dnu stranice Security Center. Pojavit će se prozor; jednostavno kliknite gumb Off. Neki vatrozidovi drugih proizvođača mogu isključiti Windows Firewall tijekom svog instaliranja.

Popis čestih pitanja (FAQ-ovi) o korištenju Microsoftovog Internet vatrozida nalazi se na www.microsoft.com/athome/security/protect/ firewall.mspx.

Detaljne informacije o konfiguriranju Windows Firewall nalaze se u 7. poglavlju "Osiguravanje Windowsa".

Automatska ažuriranja

Zlonamjerni hakeri stalno otkrivaju nove propuste u računalnim sustavima, naročito u Microsoftovim proizvodima. Svaki put kad bude pronađen neki propust, Microsoft kreira ispravak ili "zakrpu" kako bi spriječio da 'rupu' iskoriste virusi ili crvi. Ako omogućite Automatic Updates, Microsoft šalje te ispravke ili "zakrpe" na vaše računalo kada one postanu dostupne. Opcija Automatic Updates toplo se preporučuje zbog brzine nastajanja novih vrsta *malwarea*. Ako vam se ne da dohvaćati zakrpe ili ispravke za svoj operativni sustav ili ažurirati svoj antivirusni softver, značajka Automatic Updates može značajno pridonijeti onemogućivanju zlonamjernih korisnika bez stvarnog truda s vaše strane. 7. poglavlje opisuje ispravke i "zakrpe".

Zaštita od virusa

SP2 vas ne štiti od virusa, ali nadzire status antivirusnog softvera drugih proizvođača. Značajka Virus Protection govori vam je li antivirusni softver uključen i trebate li ga ažurirati. Naravno, antivirusni softverski program trebao bi vas sam upozoriti da nije ažuriran, ali nije naodmet na to vas ponovno podsjetiti. Microsoft ne podržava sve antivirusne softverske programe. One koje podržava naći ćete na adresi www.microsoft.com/security/partners/antivirus.asp. Djelomičan popis podržanih antivirusnim programa uključuje Symantec, Trend Micro, Computer Associates, GFI, F-Secure, Sophos, Kaspersky, McAfee i Panda Software.

Security Center obuhvaća i značajku Internet Options koja vam omogućuje da kreirate popise pouzdanih i ograničenih Web lokacija, podesite postavke *online* privatnosti i omogućite druge postavke sigurnosti. 7. poglavlje opisuje ove opcije.

ZoneAlarm iz ZoneLabsa

Zone Labs je kompanija za računalnu sigurnost (sada u vlasništvu CheckPoint Software Technologiesa, glavnog pružatelja sigurnosnih proizvoda tvrtkama). Kompanija proizvodi besplatan vatrozid pod nazivom ZoneAlarm koji je dostupan za preuzimanje na Web lokaciji www.zonelabs.com.

Besplatni vatrozid ZoneAlarm je vrlo zamašan softver, naročito ako uzmete u obzir da vas ne stoji ni lipe. Vatrozid ZoneAlarm provodi pet glavnih funkcija:

Firewall (vatrozid), Program Control (kontrola programa), Anti-Virus Monitoring (nadziranje antivirusne zaštite), E-mail Protection (zaštita e-pošte) i Alerts and Logs (upozorenja i dnevnici).

Funkcija Firewall

Softver vatrozida nadzire ulazne veze da bi vam pomogao u zaštiti od mogućih provalnika. Vatrozid uključuje dvije sigurnosne zone koje vam omogućuju da podesite postavke sigurnosti. Internet Zone radi sa svim računalima na Internetu. Trusted Zone kreira postavke za računala kojima vjerujete, poput onih na kućnoj mreži s kojima dijelite datoteke.

Funkcija Program Control

ZoneAlarm nadzire programe na vašem računalu koji zahtijevaju vezu s Internetom. Ovaj mehanizam izlazne zaštite pomaže u sprječavanju trojanskih konja, *spywarea* i drugog *malwarea* koji se nalazi na vašem računalu da dosegne Internet. Nakon instaliranja softvera, ZoneAlarm izdaje upozorenje svaki put kada se neki program želi povezati s Internetom. Kako vi dopuštate pouzdanim programima, poput Web pretraživača, programima za *chat*, e-poštu, tako i vatrozid automatski dopušta rad tim programima.

Funkcija Anti-Virus Monitoring

Iako besplatan vatrozid ne provodi provjeru virusa, on nadzire antivirusni softver. On vas obavještava da je antivirusni softver zastario ili da je isključen. No, to provodi samo za tri antivirusna programa: Symantecov Norton AntiVirus, McAfeeov Viruscan i EZ Antivirus Computer Associatesa. Zamijetite da većina antivirusnih programa također izvještava o potrebi za ažuriranjem antivirusnog softvera.

Funkcija E-Mail Protection

Ova značajka "zatvara u karantenu" priloge datoteka koje dolaze u porukama e-pošte. Prilozi porukama e-pošte primarna su metoda širenja virusa i crva. Besplatna verzija ZoneAlarma "zatvara u karantenu" samo priloge formata .vbs (VBS je kratica za Visual Basic Script, računalni jezik koji je bio vrlo popularan među piscima virusa, ali je ovih dana nekako izašao iz upotrebe).

Funkcija Alerts and Logs

Ova značajka provodi dvije funkcije. Alterts (upozorenja) su iskočne poruke koje od vas zahtijevaju neki odziv. Te iskočne poruke odnose se na informativna upozorenja (poput napomene da se nešto dogodilo) i na upozorenja o programima (neki program pokušava nešto provesti).

Možete odrediti da se prikazuju sva upozorenja ili samo ona vezana uz programe. Tijekom prvih nekoliko dana korištenja softvera možda ćete željeti da se prikazuju sva upozorenja. To će vam omogućiti bolje razumijevanje onoga što se događa kada koristite Internet. No, vjerojatno ćete postati zatrpani količinom upozorenja, pa se tada možete prebaciti na postavku upozorenja o programima, koja se prikazuju samo u slučaju potencijalno štetnih aktivnosti.

Dnevnici su zapisi aktivnosti vatrozida, uključujući promet koji je vatrozid blokirao. Svoje dnevnike možete pregledati klikom jahača Log Viewer u sekciji Alerts & Logs. Možete i kliknuti određeni dnevnički unos da biste dobili više informacija o nekom događaju.

3.5 Vatrozidovi koje možete kupiti

Dva smo besplatna vatrozida razmotrili dosad detaljno. Oba su prilično dobra, a možete ih pronaći i još, pretraživanjem po riječima "free personal firewalls". Kada uspoređujete besplatan vatrozid s onim koji stoji 50 američkih dolara, postoji li jedan dobar razlog da platite za vatrozid? Ako razgovaramo samo o vatrozidovima, teško bih izustio 'Da'.

Međutim, postoji jedan odličan razlog za kupnju vatrozida – mnogi se isporučuju s drugim osnovnim paketima za sigurnost na Internetu, poput antivirusnog softvera, zaštite od *spama* i detektora *spywarea*. Vatrozid ne sprječava prodor virusa koji dolaze s e-poštom niti *spam*, pa ako kupnja vatrozida znači dobivanje ovih programa za zaštitu, tada se ona isplati. Komercijalni vatrozidovi često nude više značajki i opcija od besplatnih verzija, kao što su Web privatnost, blokiranje iskočnih oglasa i sposobnost uočavanja i blokiranja poznatih crva.

Na primjer, ZoneAlarm Security Suite obuhvaća vatrozid, antivirusni softver i druge značajke kao što su zaštita od prijevara putem e-pošte i sustava za dopisivanje u realnom vremenu, zaštita privatnosti na Webu i druge značajke koji nisu uključene u besplatnu verziju.

Symantecov Norton Internet Security je još jedan skup proizvoda koji uključuje vatrozid, antivirusni softver, *anti-spyware* softver i zaštitu od pecačkih napada.

McAfeeov Internet Security Suite sastoji se od osobnog vatrozida, antivirusnog softvera, otkrivanja i uklanjanja *spywarea*, zaštite od *spama* i softver za Web privatnost.

U tablici 3.1 nalazi se popis najpopularnijih osobnih vatrozidova na tržištu. Cijene se kreću u rasponu od 39,95 do 79,95 američkih dolara (tako je bilo sredinom 2005. godine). U tablici 3.2 nalazi se popis besplatnih vatrozidova.

Tablica 3.1

Vodeći osobni vatrozidovi			
Proizvod	**Isporučitelj**	**Web Site**	**Značajke**
Black ICE PC Protection	Internet Security Systems	www.blackICE.iss.net	Vatrozid, otkrivanje provala i drugo
eTrust EZ Armor	Computer Associates	www.ca.com ili www.my-etrust.com	Vatrozid, antivirus i drugo
F-Secure Internet Security	F-Secure	www.f-secure.com	Vatrozid, antivirus, anti-spyware i drugo
Internet Security Suite	McAfee	www.mcafee.com	Vatrozid, antivirus, *anti-spam*, *anti-spyware* i drugo
Kaspersky Personal Security Suite	Kaspersky Lab	www.kaspersky.com	Vatrozid, antivirus, *anti-spam*, *anti-spyware* i drugo
Norton Internet Security	Symantec	www.symantec.com	Vatrozid, antivirus, *anti-spam*, *anti-spyware* i drugo
Panda Platinum Internet Security	Panda Software	www.pandasoftware.com	Vatrozid, antivirus, *anti-spam*, *anti-spyware* i drugo
PC-cillin Internet Security	Trend Micro	www.trendmicro.com	Vatrozid, antivirus, *anti-spam*, *anti-spyware* i drugo
Sygate Personal Firewall Pro	Sygate Technologies	www.sygate.com	Vatrozid, otkrivanje provala i drugo
ZoneAlarm Security Suite	ZoneLabs	www.zonelabs.com	Vatrozid, antivirus, zaštita e-pošte i drugo

Tablica 3.2

Besplatni vatrozidovi		
Proizvod	**Isporučitelj**	**Web lokacija**
Kerio Personal Firewall	Kerio Technologies	www.kerio.com
Sygate Personal Firewall Standard	Sygate Technologies	http://smb.sygate.com/products/spf_standard.htm
Windows XP Service Pack 2	Microsoft	www.microsoft.com/windowsxp/sp2/default.mspx
ZoneAlarm	ZoneLabs	www.zonelabs.com

Kako valja birati?

Najbolji izvori pomoći pri odabiru vatrozida jesu Internet i ljudi koje poznajete. Internet je pun recenzija, mišljenja i informacija o sigurnosnim proizvodima. Najjednostavnija metoda je da upišete naziv određenog proizvoda u tražilicu i krenete. Možda ćete morati proći preko brojnih hiperveza do tvrtke koja prodaje taj proizvod, a vjerojatno ćete naići i na druge zanimljive veze.

Za usmjerenije traženje, pogledajte *online* resurse poput CNET.com. Ova Web lokacija sadrži recenzije brojnih proizvoda za sigurnost računala, uključujući i vatrozidove. Časopisi poput *PC Magazinea* i *PC Worlda* (ili *Vidija*, *Buga* i *PC Chipa* u Hrvatskoj, op. prev.) također vam nude na svojim Web lokacijama preglede proizvoda i svoje osvrte na njih.

Druga opcija je da sami isprobate neke proizvode. Većina vatrozidova može se preuzeti s Interneta i isporučuje se s probnim rokom, uglavnom od 30 do 90 dana. Možete koristiti recenzije iz časopisa ili savjete prijatelja da biste smanjili popis na dva ili tri kandidata, te svakog od njih isprobati.

Upotrijebite probno razdoblje da otkrijete koji vam proizvod najviše odgovara. Koji je najisplativiji? Koji ima najjasnije i najprivlačnije sučelje? S kojim se osjećate najudobnije? Koji vatrozid najbolje upozorava? S kojim se vatrozidom osjećate najsigurnije? Koji ima najbolje boje? Koji su god vaši određeni kriteriji, možete ih testirati do mile volje. Zapravo, ako želite odvojiti dosta vremena za preuzimanje s Interneta, vjerojatno ćete moći godinu dana besplatno koristiti softver mijenjajuću jednu probnu verziju za drugu.

3.6 Testiranje vatrozidova

Kako ćete znati radi li vaš vatrozid? Jedan način da to saznate je da ga testirate. Na raspolaganju imate brojne lokacija na Internetu koje skeniraju vaše računalo i izvještavaju vas o rezultatima. Slijedi popis nekoliko dobrih lokacija koje će vam pomoći da vidite kako vaše računalo izgleda izvana.

ShieldsUP! (www.grc.com)

Ova lokacija, koju vodi guru Steve Gibson, godinama skenira računala korisnika (uz njihova dopuštenja, naravno). To je odličan način provjere nekih uobičajenih ranjivosti poput dijeljenja Windows datoteka preko NetBIOS-a i portova koji se mogu otvoriti (i tako postati dostupni zločestim dečkima). Dobivene je rezultate lako razumjeti. Lokacija obuhvaća i veze do više informacija o osobnim vatrozidovima te sigurnosti računala.

Lokacija nudi razne testove. Dva su posebno korisna za kućne korisnike. Prvi se zove Common Ports i provjerava 26 često korištenih portova koji mogu biti otvoreni (i zbog toga biti pristupačni huliganima). Drugi test zove se Service Ports i provjerava 1056 portova. Ovaj je test opsežniji i traje malo dulje.

Druge lokacije za testiranje mogu provoditi slična testiranja, ali ni jedna to ne čini s Gibsonovim užitkom i entuzijazmom. Ako testirate svoj vatrozid da biste vidjeli kako djeluje na potencijalne provalnike s Interneta, tada bi ova lokacija trebala biti vaša prva stanica.

Symantec Security Check (www.symantec.com/homecomputing/)

Symantec Security Check skenira vaše računalo zbog raznih potencijalnih ranjivih točaka, uključujući portove koji mogu odgovoriti na nepoželjne zahtjeve, prisutnost programa trojanskih konja te izvodi li se antivirusni softver. Rezultati testiranja su razumljivi (iako mnogo suhoparniji od Gibsonovih), a detaljni su rezultati dostupni za Hacker Test (koji prikazuje portove koji odgovaraju ili ne odgovaraju na zahtjeve za uspostavljanje veze). Ova provjera zahtijeva preuzimanje ActiveX-a da bi funkcionirala.

McAfee MySecurityStatus (http://us.mcafee.com/MySecurityStatus/)

Poput Symantec Security Checka, MySecurityStatus zahtijeva preuzimanje ActiveX-a da bi mogao provjeriti status vašeg osobnog vatrozida i antivirusnog softvera.

PivX PreView (www.pivx.com/preview)

PreView je besplatan sigurnosni alat koji je dostupan za preuzimanje s Interneta, u vlasništvu kompanije PivX. Ovaj alat daje ocjenu za sigurnost vašeg računala na temelju četiri kategorije: Threat Center, Security Software, Patches/HotFixes i Firewall Protection. PreView analizira vaše računalo da bi proračunao rezultat sigurnosti koristeći četiri kategorije. On je jednostavan način za izražavanje stupnja ranjivosti vašeg računala na napade. Međutim, značajan dio vaše ocjene nosi činjenica jeste li kupili neki drugi proizvod PivX-a, pa ocjenu protumačite s malom zadrškom.

Alat ima razne funkcije (koje su detaljnije opisane u 7. poglavlju), od kojih jedna provodi osnovnu probu vašeg vatrozida. Ona s Interneta skenira vaše računalo da vidi koji su portovi otvoreni i odazivaju se na nepoželjne zahtjeve.

Da biste pokrenuli skeniranje, kliknite ikonu Firewall Protection. Prije samog pokretanja morat ćete prihvatiti uvjete pod kojima se skeniranje provodi. Uvjeti načelno žele provjeriti da ste vi vlasnik računala te da dozvoljavate ovaj zahtjev. Vaš bi vas vatrozid, kada pokrenete skeniranje, mogao upozoriti da izvršivi PreView pokušava uspostaviti vezu s Internetom. To je u redu, pa akciju možete odobriti.

Skeniranje provjerava 16 uobičajenih portova, uključujući port 80 (za Web) i port 25 (za SMTP, protokol za slanje e-pošte). Izvještaj prikazuje status svakog porta (otvoren ili zatvoren) i njegovu uobičajenu namjenu. Ako se vaš vatrozid izvodi u modu Stealth, tada biste trebali dobiti visoku ocjenu. Zapamtite da je zatvoreni port idealan. To ne znači da se vaš Web pretraživač neće povezati s Webom; to jednostavno znači da vaš vatrozid neće reagirati na nepoželjne pokušaje otvaranja komunikacijskog kanala.

AuditMyPC (www.auditmypc.com)

Ova lokacija provjerava dostupne portove na vašem stroju. Ona može skenirati u potrazi za *spywareom* i ranjivim točkama Web pretraživača. Rezultati nisu toliko informativni kao oni koje smo već spomenuli, ali vam lokacija omogućuje da skenirate svih 65 535 portova umjesto podskupa onih koji najčešće zlorabe provalnici. Ona vam omogućuje i testiranje odabranih portova.

3.7 Popis za provjeru

Upotrijebite popis za provjeru kao brzi referentni vodič za sadržaj iznesen u ovom poglavlju.

Učinite

- Instalirajte vatrozid na svoje računalo i upotrijebite postavku "stealth".
- Nabavite Windows XP Service Pack 2 (www.microsoft.com/windowsxp/sp2/default.mspx; www.microsoft.com/croatia).
- Pažljivo razmotrite korištenje vatrozida koji obuhvaća antivirusne, *anti-spyware* i druge sposobnosti.
- Testirajte svoj vatrozid pomoću jedne ili više lokacija popisanih u odjeljku "Testiranje vatrozidova"
- Kod isporučitelja vatrozida redovito provjeravajte postoje li ažurirane verzije softvera.
- Redovito kreirajte sigurnosne kopije važnih datoteka.

Nemojte učiniti

- Nemojte koristiti Internet bez vatrozida.
- Nemojte vjerovati da će vas vatrozid zaštititi od svih rizika koji dolaze s Interneta.

3.8 Korisni izvori

RTFM. Ovo je skraćeno od *Read the f..... manual* (pročitaj j..... priručnik, op. prev.). Na brojna pitanja možete dobiti odgovore u priručniku koji se isporučuje s proizvodom ili na *online* FAQ lokacijama. Ako na *online* lokacijama za pomoć postavite jednostavna pitanja, nemojte se čuditi ako kao odgovor dobijete RTFM preporuku.

Web lokacija www.firewallguide.com izvrstan je izvor ako kupujete softver ili hardver za zaštitu. Na njoj se nalaze tone informacija o vatrozidovima i drugim rješenjima kao što su antivirusni i *anti-spyware* alati. Lokacija također sakuplja članke iz popularnih časopisa za računala uključujući i recenzije te usporedbe proizvoda za kućnu sigurnost.

Secretes and Lies: Digital Security in Networking World (Tajne i laži: digitalna sigurnost u umreženom svijetu) autora Brucea Scheinera. Ova knjiga daje odličan pregled računalne sigurnosti, uključujući vatrozidove, iako se ne radi o priručniku. On govori i o faktoru ljudske slabosti u osnovi svakog sustava zaštite (uključujući i stalno lamentiranje stručnjaka za sigurnost kako je najbolja zaštita na svijetu bespomoćna kada se radi o ljudima koji kliknu na prilog u poruci e-pošte). Knjiga razmatra složene teme s humorom i razumljivim jezikom.

4. poglavlje

Kako se riješiti nepoželjnih gostiju? 1. dio: Virusi i crvi

U knjizi koristimo pojam *malware* (kratica od MALicious softWARE; zlonamjerni softver). To je općenit pojam koji opisuje programski kôd kreiran s namjerom da našteti vašem računalom sustavu. *Malware* obuhvaća brojni zlonamjerni softver, uključujući viruse, crve, trojanske konje i neki *spyware* i *adware* visokog rizika.

Ovo poglavlje ispituje razloge koji leže ispod nevjerojatnog porasta *malwarea.* Ono također opisuje dvije specifične vrste *malwarea*: viruse i crve. Objasnit ćemo kako oni mogu dospjeti na vaše računalo i koje korake možete poduzeti da se zaštitite. Navest ćemo jake i slabe strane antivirusnog softvera te objasniti kako možete blokirati i/ili ukloniti viruse i crve.

4.1 Porast *malwarea*

Malware cvjeta iz nekoliko razloga. Prvi je rastuća komunikacijska sposobnost računala. U starim danima (kasne1980-te), *malware* je putovao na disketama; da biste uhvatili virus trebali ste zaraženu disketu umetnuti u svoje računalo. Kako je Internet narastao, *malware* je počeo "jahati" na raznim komunikacijskim mehanizmima. Danas se *malware* širi e-poštom, sustavima za dopisivanje u realnom vremenu, raznim Internet protokolima i World Wide Webom.

Drugi razloga procvata *malwarea* je rastuća homogenizacija naših računalnih okruženja. *Malware* napisan za jedan operativni sustav ili platformu zasnovanu na nekom čipu ne može funkcionirati na drugim sustavima i platformama. U početku je ova nekompatibilnost predstavljala barijeru za zarazu, jer su se tada na računalima izvodili razni operativni sustavi. Danas, međutim, ta se raznolikost svela na dva sustava: Microsoft Windows i UNIX (uključujući i varijante poput Linuxa). Na vrhu su uobičajene aplikacije kao što je programski paket Microsoft Office i Web pretraživači koji rade na višestrukim operativnim sustavima. *Malware* koristi slabu zaštitu tih operativnih sustava i aplikacijskog softvera kao sredstva za inficiranje računalnog sustava. Kada kombinirate homogenost računalnog okruženja s brojnošću smjerova iz kojih prijeti zaraza na Mreži, rezultat je epidemija koja zahvaća kućna i poslovna računala i Internet.

Treći razlog cvjetanja *malwarea* je taj da su tradicionalni obrambeni alati za *malware* reaktivni. Antivirusni i *anti-spyware* softver najefikasniji je protiv poznatih napada. No, kad se pojavi novi *malware*, na raspolaganju za slobodno širenje stoji mu vremensko razdoblje potrebno da stručnjaci za zaštitu računala analiziraju napad, pripreme lijek i distribuiraju ga. Zločesti dečki su u prednosti koju naravno koriste. Vatrozidovi mogu blokirati neuobičajene komunikacijske kanale, ali velik dio korisnika Interneta nema vatrozid, ili ima vatrozid koji nije ispravno konfiguriran. Napadači također koriste uobičajene kanale kao što su Web ili e-pošta za širenje *malwarea*. Neke su tehnologije tako razvijene da mogu otkriti i blokirati nove i nepoznate napade, ali još uvijek nisu spremna za korištenje; često uzrokuju probleme s legitimnim programima i aplikacijama.

Četvrti razlog koji najviše zabrinjava je da *malware* cvjeta zbog novca. Udruge kriminalaca i poslovne organizacije bez reputacije stječu profite pisanjem programa koje ne biste željeli na svojem računalu. Prije se pretpostavljalo da pisce *malwarea* motivira neprijateljsko ponašanje prema društvu; oni su pisali zlonamjerne programe da bi dobili pohvale istomišljenika ili da bi stekli samopouzdanje "pumpanjem" vlastitog ega. Širenje epidemije *malwarea* pribavlja neku vrstu slave u računalnom podzemlju, kao što to nekoj rock zvijezdi pribavlja snimka hita ili nekom piscu *best seller*. (Ako vas zanimaju detalji o ovoj temi pročitajte istraživanje Sarah Gordon na adresi www.badguys.org/papers.htm.)

Ali injekcija novca u ovoj jednadžbi mijenja sliku. Pisci *malwarea* koji rade za novac ne žele slavu. Oni kreiraju tihe ili nevidljive programe koji se ubacuju na strojeve i na njima ostaju što je dulje moguće. *Malware* koji dobiva publicitet u medijima je *malware* koji se lovi i uklanja. *Malware* koji generira profit nastoji ostati skriven.

Postoje tri načina na koja se može zaraditi novac pisanjem i širenjem zlonamjernog softvera. Prvi je špijunaža. Korporacije i vlade stalni su ciljevi špijuna koji su plaćeni za krađu državnih tajni ili intelektualnog vlasništva. (Na primjer, u svibnju 2005. godine objavljeno je da su izvršni direktori u tri izraelske tvrtke uhićeni zbog unajmljivanja privatnih istražitelja za špijuniranje konkurencije. Privatni su istražitelji koristili trojanske konje za krađu datoteka i dokumenata sa zaraženih računala. U jednom starijem slučaju, haker je upotrijebio QAZ Worma da dobije pristup nekom Microsoftovom izvornom kodu u 2000. godini.) Zlonamjerni programi kao što su *keystroke loggers* i *rootkits* dio su digitalnog špijunskog *tradecrafta*. (*Rootkits* su programi koji prebivaju duboko unutar operativnog sustava računala i napadaču pružaju potpunu kontrolu nad tim računalom. Napadač se po želji može vratiti na zaraženo računalo i pokrenuti bilo koju operaciju. Dobro ukopani *rootkits* mogu se sakriti i od računalnih administratora s dugogodišnjim iskustvom. Da bi ih se otkrilo i uklonilo potrebni su forenzički alati.) Iako digitalna špijunaža postoji toliko dugo koliko i računala, *rootkits* nisu samo alati elitnih operativaca; unaprijed ugrađeni *rootkits* mogu se nalaziti na Internetu.

Drugi je da osoba može zaraditi novac korištenjem *malwarea* za kompromitiranje a potom iznajmljivanje velikog broja računala *spamerima*, *scamerima* i iznuđivačima. Automatizirani *malware* može otkriti, provaliti ili preuzeti kontrolu nad tisućama računala i od njih napraviti vojsku strojeva-robova kojima se može upravljati na daljinu. Ti strojevi-robovi koji se nazivaju i zombiji ili larve, tada se mogu iznajmljivati drugima, koji će ih koristiti za slanje *spama* ili pokretanje DoS napada. (DoS napad preplavljuje ciljnu lokaciju s toliko mnogo prometa da legitimni korisnici ne mogu dobiti pristup.) Kućna računala s DSL ili kabelskim modemima su popularne mete jer su često nezaštićena, a njihove širokopojasne internetske veze znače da mogu slati tisuće poruka e-pošte ili zatrpati tisuće Web lokacija u sekundi. *Spameri* (a od nedavno i *phisheri*) mogu unajmljivati te mreže-larve za širenje najnovije runde *scam* poruka. Udruge kriminalaca koriste larve za iznuđivanje novca od *online* pornografskih i lokacija za kockanje, tako da prijete kako će DoS napadima lokaciju dovesti do bankrota. Stručnjaci za zaštitu tvrde da kriminalci mogu ciljati i legitimnije tvrtke.

Treći način stvaranja profita od *malwarea* jest krađom provedenom *spywareom*, ili oglašavanjem generiranim *adwareom* visokog rizika. *Spyware* kao što su *keystroke loggers* može bilježiti osjetljive informacije poput *online* ID-a bankovnog

računa i lozinke te ih slati napadaču koji potom može prenijeti novac s vašeg računa. *Adware* programi koriste isporuku oglasa na vaš PC. U nekim slučajevima, ti programi mogu skupljati informacije s vašeg računala, uključujući informacije koje se odnose na korištenje Web pretraživača na Internetu ili navike rada na računalu, koje zatim šalju na udaljeno računalo ili drugu lokaciju u cyberprostoru. Kompanije plaćaju tvrtkama koje se služe *adwareom* da generiraju iskočne oglase ako posjetite lokaciju njihovog konkurenta ili lokacije koje su u vezi s proizvodom ili uslugom koje prodaju. *Adware* može domaću tvrtku izvještavati i o vašem surfanju, koja skuplja i preprodaje informacije kao "istraživanja potrošača". Dok je jasno da su programi poput trojanskih konja ili virusa zlonamjerni (i u mnogo slučajeva nelegalni), *adware* zauzima sivo područje. Mnogo *adwarea* koji cirkulira Internetom kreiraju tvrtke (za razliku od udruga kriminalaca ili slobodnih programera). Te tvrtke imaju popis tvrtki-klijenata koje koriste njihove usluge za oglašavanje ili istraživanje tržišta, te imaju svoju marku i reputaciju da ih štite, vrlo slično bilo kojoj drugoj tvrtki. (O *adwareu* detaljno govorimo u 5. poglavlju "Kako se riješiti nepoželjnih gostiju?, 2. dio: *spyware*, *adware* i trojanski konji".)

Svrha svega izloženog je da pokažemo kako je *malware* ozbiljan problem koji će unedogled inficirati korisnike. Poznavanje prijetećeg okruženja u kojem radite znači da ste u stanju poduzeti korake da biste se zaštitili. Nije nam cilj da vaše računalo učinimo neranjivim; to jednostavno nije moguće. Međutim, Internet je pun lakih meta. Naš je cilj da vas učinimo težom metom.

4.2 Virusi i crvi

Virus je program ili kod koji se sam replicira u drugim datotekama s kojima dolazi u kontakt. Virus može zaraziti drugi program, sektor za podizanje računala, particiju ili dokument koji podržava makronaredbe, tako da se umetne ili prikvači za taj medij. Većina virusa samo se razmnožava, ali mnogi mogu oštetiti vaš računalni sustav ili korisničke podatke (ta se sposobnost virusa naziva *payload*). Ponekad virus zahtijeva interakciju čovjeka da bi se replicirao, poput klika programa koji sadrži virus ili otvaranja neke zaražene datoteke. Kada se jednom aktivira, virus može kreirati i distribuirati svoje kopije inficirajući druge programe ili se širiti komunikacijskim mehanizmima poput e-pošte. Tablica 4.1 sadrži detaljnije informacije o pojedinim vrstama virusa.

Crvi su programi koji omogućuju distribuciju vlastitih kopija, često bez interakcije čovjeka. Crv može oštetiti ili kompromitirati sigurnost računala. On može stići koristeći ranjivosti sustava ili kada korisnik otvori neku zaraženu poruku e-pošte

Tablica 4.1

Terminologija za viruse

Vrsta	Primjeri	Opis
Virus koji inficira datoteke	Cascade	Virusi koji inficiraju datoteke sami se kvače za programe, izvršne datoteke i skripte. Ako se na računalu izvodi zaražena datoteka, virus se može širiti na druge programe.
Makro virus	Melissa, Concep	Makronaredbe su mali programi koji postoje unutar većih aplikacija kao što je Microsoft Word. Makronaredbe se mogu napisati da bi se pojednostavili uobičajeni zadaci. Makro virusi mogu sami sebe kopirati, brisati ili mijenjati dokumente i provoditi druge nepoželjne funkcije.
Virus sektora za podizanje računala	Michelangelo	Sektor za podizanje diska ili tvrdog diska upućuje računalo koje programe pokrenuti kada se disk pročita ili kako pokrenuti operativni sustav. Virusi sektora za podizanje izvršavaju se svaki put kada se odnosni disk koristi ili kada se uključi računalo.
Virus rezidentan u memoriji	Jerusalem	Virus koji ostaje u memoriji računala nakon aktiviranja koda virusa.
Polimorfni virus	Marburg, Zmist	Virus koji može promijeniti uzorak svojih bajtova kada se replicira, čime sprječava otkrivanje pomoću jednostavnih tehnika za skeniranje stringova.
Retro virus	Gobi	Virus koji aktivno napada antivirusni program ili programe da bi spriječio otkrivanje.

ili klikne na prilog. Za razliku od virusa, crvi ne inficiraju datoteke domaćina. Oni su izgrađeni kao samodostatni programi koji rade nezavisno od drugih programa na računalu. Uz korištenje transporta kao što je e-pošta ili sustav za dopisivanje u realnom vremenu, neki crvi imaju ugrađene mehanizme koji im omogućuju širenje putem Interneta i lokalnih mreža. Tablica 4.2 sadrži više informacija o crvima.

Današnji se crvi sve više kreiraju za traženje i iskorištavanje specifičnih pukotina u popularnim operativnim sustavima ili aplikacijama. Te pukotine koje nazivamo i ranjivosti dopuštaju crvima da dobiju pristup računalu, provedu bilo koji zadatak koji im je dodijeljen i repliciraju se da bi pronašli druga ranjiva računala. Ponekad

Tablica 4.2

Terminologija za crve

Vrsta	Primjeri	Opis
Crv	Bugbea, Netsky, MyDoom	Crv je program koji radi i omogućuje distribuciju vlastitih kopija s jednog na drugi disk ili kopira sebe koristeći se e-poštom ili drugim mehanizmima transporta. Crv može oštetiti i kompromitirati sigurnost računala. Može doći preko eksploatacije ranjivosti sustava ili klikom na neku zaraženu poruku e-pošte.
Mailer i mass-mailer crv	LoveLetter (mass mailer), Happy99 (mailer)	Mailer i mass-mailer crvi posebna su klasa računalnih crva koji se sami šalju e-poštom. Mass maileri šalju višestruke vlastite kopije dok maileri rjeđe šalju sami sebe.
Miješane prijetnje	Nimda, Slammer, Blaster	Miješane prijetnje kombiniraju karakteristike virusa, crva i trojanskih konja s ranjivosti softvera za pokretanje, prijenos i širenje napada. Karakteristike miješanih prijetnji uključuju njihovu sposobnost da nanesu štetu, da se razmnožavaju raznim metodama i napadaju višestruke točke, potencijalno se šireći bez intervencije čovjeka i iskorištavanja ranjivosti softvera. Korištenjem višestrukih metoda i tehnika miješane prijetnje mogu se brzo širiti i uzrokovati veliku štetu.

su proizvođači softvera svjesni ranjivosti, pa izdaju ažurirane verzije softvera koje se nazivaju i sigurnosne zakrpe. U nekim slučajevima proizvođač softvera ne zna za ranjivost dok se ne pojavi novi crv ili drugi *malware* koji počne plaziti Internetom pa tek tada proizvođač brzo izdaje ispravak. U svakom slučaju, obaveza je krajnjeg korisnika (vas) da pronađe i primijeni zakrpe. Jedan od razloga zbog kojeg su crvi tako uspješni je taj da korisnici i tvrtke nisu baš dobri u krpanju svojih računala. Detalje o sigurnosnim zakrpama naći ćete u 7. poglavlju "Osiguravanje Windowsa".

Kao što smo napomenuli, crvi se rijetko oslanjaju na interakciju čovjeka. Ako crv može uspostaviti mrežnu vezu s vašim računalom koje ima specifične pukotine koje taj crv traži, a vi nemate instaliranu zaštitu, igra je uglavnom gotova.

Što crvi i virusi mogu učiniti?

Crvi i virusi kreirani su za prijenos *payloada* (zlonamjernog računalnog koda) na ciljno računalo. Taj *payload* je kreiran za provođenje specifičnih funkcija kao što su brisanje ili promjena podataka, instaliranje softvera na vaše računalo ili kreiranje stražnjih vrata koja napadač može kasnije upotrijebiti da bi dobio neovlašten pristup vašem računalu.

Internet crvi i virusi stvaraju probleme inficiranim strojevima, ali crvi mogu napraviti veću popratnu štetu zbog mrežnog prometa koji generiraju prilikom širenja Internetom. Pogledajmo, primjerice, SQL Slammer, brzo pokretni crv koji je ciljao poslužitelje na kojima se izvodila ranjiva verzija Microsoft SQL Server 2000 softvera. (SQL je kratica od *Structured Query Language,* jezika koji se koristi u bazama podataka.) Lansiran u siječnju 2003. godine, crv SQL Slammer u trenu je preuzeo kontrolu nad ranjivim strojevima i počeo tražiti nove žrtve. Na vrhuncu brzine njegova širenja crv je udvostručavao broj strojeva pod svojom kontrolom svakih 8,5 sekundi. Rezultirajuća plima prometa koju su generirala kompromitirana računala dovela je Internet u stanje mirovanja. Veći je dio Sjeverne Koreje izgubio pristup Internetu, Continental Airlines morala je otkazati letove sa svojeg uzletišta u Newarku, a brojni su bankomati prestali raditi na nekoliko sati.

Crvi i virusi postoje i u jednostavnim oblicima, ali su se u posljednjih nekoliko godina počeli križati da bi kreirali miješane prijetnje uz različite načine širenja. Na primjer, mnogi crvi (koji se nazivaju *mass maileri*) šire se sami e-poštom. Drugi crvi koriste razne mehanizme širenja.

Dobar je primjer crv Nimda, koji se pojavio 18. rujna 2001. godine. Taj je crv koristio pet različitih metoda širenja. Prva je bila skeniranje Windows poslužitelja na kojima su se izvodile ranjive verzije IIS-a (IIS je kratica od *Internet Information Server* što je Microsoftov softver za Web poslužitelj). Kada se odlučio za neki poslužitelj, upotrijebio ga je kao lansiranu rampu za traženje drugih ranjivih strojeva. Širio se i putem Outlooka (Microsoftovog klijenta za e-poštu), šaljući se na adrese iz žrtvina adresara. Nimda se instalirao i na računala ljudi koji su dolazili na neki Web poslužitelj zaražen Nimda crvom; vlastiti je kod snimao putem Internet Explorera (Microsoftov pretraživač). Nimda se širio i kroz Windows File Sharing (Microsoftov mehanizam za dijeljenje datoteka između računala) te kroz postojeća stražnja vrata koja su prije instalirali crvi koji su napali Windows IIS poslužitelje.

4.3 Antivirusni softver

Svoje računalo možete na razne načine zaštiti od zaraze virusima i crvima. Najbolja zaštita od virusa i crva je antivirusni (AV) softver. AV softver može spriječiti instaliranje virusa, a može i otkriti, izolirati i ukloniti viruse i crve s vašeg računala koji su se provukli kroz obrambene mehanizme.

Tradicionalni AV softver radi stvaranjem potpisa svakog virusa ili komada *malwarea*. Potpis identificira sekciju koda koja se pojavljuje samo u *malwareu*. Zato je potpis poput otiska prsta – on predstavlja strogu evidenciju identiteta programa. Svaki put kada vaš AV softver skenira neki prilog u e-pošti ili ispituje datoteke na tvrdom disku, on traži otiske prsta poznatih virusa i crva.

Što AV softver može učiniti?

AV vas može zaštiti od poznatih virusa koji se pojavljuju na nekoliko mjesta: u dolaznoj i odlaznoj e-pošti, porukama u sustavu za dopisivanje u realnom vremenu i na tvrdom disku vašeg računala. Svoj biste AV softver trebali konfigurirati da on automatski skenira izlazne i ulazne poruke e-pošte. (MSN koristi proizvode za skeniranje virusa od tvrtke Trend Micro, Yahoo! koristi Norton AntiVirus, a AOL koristi McAfee.)

Većina antivirusnih proizvoda isporučuje se sa skenerom u realnom vremenu koji provjerava vaše datoteke svaki put kada im pristupate. Trebali biste i redovito skenirati svoj tvrdi disk u potrazi za *malwareom* koji se možda nastanio na vašem PC-u. Većina AV softvera provodi skeniranja prema nekom vremenskom rasporedu, u redovitim intervalima, ali ona mogu potrajati (potpuno skeniranje mojeg prijenosnog računala traje oko 90 minuta) i usporiti ostale aplikacije. Možete prekinuti vremenski raspoređeno skeniranje ako vam ono usporava rad, ali svakako provodite potpuno skeniranje što je češće moguće. Neki stručnjaci savjetuju da je skeniranje potrebno provesti jednom tjedno, ali ja mislim da samo ljudi s jakim higijenskim navikama (ili paranoici) to zapravo rade tako često. Ako uspijete pustiti skeniranje jednom mjesečno, to bi vam trebalo omogućiti da ostanete u dobroj formi.

Što AV softver ne može učiniti?

Mehanizmi zaštite tradicionalnog AV softvera ne mogu vas zaštiti od virusa za koje proizvođači AV softvera ne znaju. Kao što ste možda i sami zaključili iz odlomka o potpisima, mana otkrivanja potpisa je ta da AV tvrtka mora imati

kopiju virusa kako bi kreirala potpis. Kod potpuno novih virusa koje nikada prije nitko nije vidio AV softver neće pomoći. Novi *malware* dobiva slobodan prolaz dok AV tvrtke ne uspiju analizirati *malware*, kreirati potpis, testirati ga i distribuirati svojim klijentima. To se obično rješava unutar 3 do 4 sata nakon provale, ali ako nemate sreće i postali ste jedna od prvih zaraženih žrtava, trebat ćete pričekati dok vaš proizvođač ne izda pomoćni program za uklanjanje tog *malwarea*. (Detalje potražite u okviru na kraju ovog poglavlja "Uklanjanje varijante crva Beagle".)

Postoje tehnologije koje nastoje zaustaviti nepoznati *malware* ispitivanjem ponašanja softvera koje bi upućivalo na to da će on računalu učiniti nešto štetno ili nepoželjno. Na primjer, mnogi AV proizvodi uključuju heurističke mehanizme koji traže karakteristike slične makro-virusima unutar koda. Taj isti kod bio bi neefikasan u otkrivanju Windows-temeljenih trojanskih konja ili crva. Heuristički mehanizmi dokazali su se efikasnima u pronalaženju varijanti poznatog *malwarea* ili polimorfnih virusa. Varijante su promjene provedene u nekom poznatom *malware* programu koje pomažu pri skrivanju od detekcije pomoću potpisa, promjene u napadačkom *payloadu*, ili promjene u načinu rada sustava uzrokovane zlonamjernim kodom. Današnji crvi često uključuju stotine ili tisuće varijanti koje su izdane ubrzo nakon originalnog napada. Polimorfni virusi su programirani da mijenjaju svoj kod u redovitim vremenskim intervalima kako bi umakli skeniranju temeljenom na potpisu i dalje nastavili sa svojim djelovanjem.

Premda heuristička detekcija može biti vrlo efikasna protiv određenih klasa nepoznatih prijetnji, ona ne pokriva sve vrste prijetnji. Druga tehnologija, *Host Intrusion Prevention Solutions (HIPS)*, također može zaustavljati nepoznate napade ispitivanjem koda na zlonamjerno ponašanje. Ova tehnologija također zaustavlja prelijevanje međumemorije, uobičajen napad koji koristi *malware*. Prelijevanje međumemorije šalje više podataka na neko područje u memoriji računala (koje se naziva međumemorija) nego što računalo očekuje. U ovoj vrsti napada, dodatni podaci obično su napadački kod koji napadaču daje kontrolu nad strojem. Prelijevanja međumemorije tipično koriste crvi, uključujući crv Code Red, Nimda i Sasser.

HIPS tehnologija je važan napredak u sigurnosti jer je ona proaktivna; odnosno, računalo je zaštićeno do nepoznatih napada bez potrebe za čekanjem isporuke novog potpisa. Proaktivna tehnologija je sve više potrebna jer se novi napadi vrlo brzo pojavljuju i mogu zlorabiti tisuće ili čak i stotine tisuća žrtava prije nego što se razviju potpisi.

Uz navedeno, glavni nedostatak HIPS tehnologije je to što često griješi i nastoji spriječiti funkcioniranje legitimnih programa. Kada se to dogodi, to se naziva lažna pozitivnost *(false positive)*. Lažna pozitivnost muči već godinama detekcijsku tehnologiju i glavni je razlog da tehnologija temeljena na potpisu još uvijek postoji – iako je reaktivna, ona je točna.

Uz to, većina HIPS tehnologije namijenjena je korporativnim okruženjima, u kojima administrator mreže bolje razumije i definira smjernice sigurnosti koje određuju kako će HIPS rješenje raditi. S vremenom će zasigurno ove tehnologije postati bolje shvaćene, te će se pojaviti proizvodi više orijentirani korisnicima. Brojni proizvodi za sigurnost postaju dostupni, uključujući HIPS tehnologije kao što je zaštita od prelijevanja međumemorije. Primjer jednog takvog rješenja je TruPrevent Personal iz tvrtke Panda Software. Ono je dizajnirano kao dopuna AV proizvodima jer je njezin cilj otkriti napade koji nemaju potpise. Ako vas zanima ova tehnologija, tvrtka Panda Software daje vam da probate TruPrevent prije nego što ga kupite. Preporučujem vam da iskoristite probni rok da biste vidjeli stvara li softver probleme kod normalnih računalnih funkcija.

4.4 Ostale metode zaštite

AV softver ne može vas uvijek zaštititi od crva koji se šire putevima različitim od e-pošte ili sustava za dopisivanje u realnom vremenu. AV softver može pronaći crve (ili drugi *malware* koji crvi dostavljaju na ciljna računala) prilikom skeniranja tvrdog diska. Ali da bi ih se spriječilo da uopće napadnu vaš stroj trebate poduzeti korake koji su opisani u ostatku ovog poglavlja.

Upotrijebite vatrozid

Kao što je opisano u 3. poglavlju "Vatrozidovi", vatrozid može sakriti vaše računalo od drugih računala na Internetu. Kada imate ispravno konfiguriran vatrozid, crvi koji skeniraju Internet u potrazi za ranjivim računalima jednostavno preskaču vaš stroj. Razmotrite korištenje sigurnosnog softvera koji obuhvaća višestruke značajke u jednom proizvodu, uključujući AV softver, vatrozid, *anti-spyware* softver itd. Neki AV i softveri vatrozida uključuju i otkrivanja provala i prevencijsku tehnologiju, koja pregledava ulazni promet s Interneta da bi otkrila potpise poznatih crva i drugog *malwarea*. Na primjer, Norton AntiVirus uključuje osnovne

sposobnosti detekcije provala i njihovog sprječavanja. Softver za detekciju provala i njihovo sprječavanje može blokirati svaki *malware* čiji potpis softver ima i pruža zaštitu za neke ranjivosti operativnog sustava za koje još ne postoji poznata eksploatacija i kod *malwarea*. Sposobnosti detekcije provala i njihovog sprječavanja dodaju još jednu razinu zaštite kod rizika u vezi sigurnosti.

Ne otvarajte neobične poruke e-pošte

E-pošta je najbolje što se dogodilo računalnim virusima od pojave računala. E-pošta pruža komunikacijski mehanizam za širenje virusa, ima popis novih domaćina za zarazu (sve adrese u vašem adresaru) i dopušta kreatoru virusa da, s malo društvenog inženjeringa, navede ljude na otvaranje poruka čime se omogućuje širenje virusa. To je razlog zbog kojeg biste trebali biti pažljivi prilikom pregledavanja poruka u svojem poštanskom sandučiću. Ako vidite da poruka dolazi od nekoga koga ne poznajete, ispitajte je ne biste li pronašli sljedeće znakove:

- Ima li adresa u polju From: nepoznato ime, čudnu strukturu ili nepoznatu domenu? (Domena je informacija s desne strane znaka @.)
- Sadrži li redak Subject: nasumične znakove umjesto teksta? (To znači da je poruka e-pošte pisana na jeziku koji vaš klijent za e-poštu ne podržava, pa ne može ispravno renderirati strani tekst.) Još jedan znak upozorenja je prazan redak Subject:.
- Zvuči li redak Subject: kao *spam*? (Mnogi *spameri* i *phisheri* regrutiraju pisce virusa da uključe *malware* u njihovu *junk* poštu kao neku vrstu bonusa. *Malware* može provoditi sve vrste funkcija, od bilježenja vaših pritisaka na tipke do pretvaranja vašeg računala u potencijalnu *spam* larvu.)
- Jeste li primili nekoliko poruka e-pošte od istog pošiljatelja koje imaju sumnjivo slične retke Subject?

Ako možete potvrdno odgovoriti na jedno od tih pitanja, tada bi bilo najbolje da te poruke izbrišete bez otvaranja. To vam savjetujemo zato jer se *malware* aktivira kada otvorite poruku e-pošte. Ne želite li izbrisati poruku, ne otvarajte je dan ili dva. Upotrijebite to vrijeme da na Web lokaciji proizvođača svojeg AV softvera provjerite upozorenja o napadima novih virusa ili crva. Ta upozorenja često uključuju informacije koje će vam pomoći da prepoznate virus u svojem poštanskom sandučiću, poput navoda u retku Subject: koji koristi pisac virusa.

Nemojte kliknuti na veze ili programe unutar poruka e-pošte

Ako ipak otvorite neobičnu poruku, nemojte kliknuti ni na jednu vezu ili program koji se nalazi u poruci. Čak i ako poznajete osobu koju vam je poslala poruku, ona bi mogla biti žrtva virusa. *Mass-mailer* virusi i crvi kradu adresare žrtava kako bi se slali što je moguće većem broju drugih žrtava, dijelom zato jer se time iskorištava povjerenje između korespondenata. Ako sumnjate na vezu koju vam je poslao netko koga poznajete, upotrijebite drugu metodu, kao što je telefonski poziv da biste se uvjerili kako je pošiljatelj stvarno poslao poruku e-pošte i da se veza ili program u toj poruci mogu upotrijebiti. Druga opcija je da ponovo upišete vezu izravno u svoj pretražitelj umjesto da kliknete na vezu. Tako ćete znati da niste povezani s zlonamjernom Web lokacijom, ako veza sadrži skrivene znakove.

Ažurirajte svoj softver

Novi se virusi i crvi stalno kreiraju, pa morate redovito ažurirati svoj AV softver. Ako vaš AV softver podržava automatsko ažuriranje, tu biste opciju trebali odabrati, jer se novi potpisi i druga ažuriranja isporučuju na vaše računalo bez vašeg sudjelovanja. Na primjer, u Norton AntiVirusu možete uključiti opciju Automatic LiveUpdate, uslugu koja šalje najnovije definicije virusa i ažurirane programe na vaše računalo svaki put kada se povežete na Internet.

Možete također odabrati da vas Norton svaki put kada je dostupna ažurirana verzija pita želite li da je automatski primijeni na vaše računalo. Ako više volite sami preuzimati ažurirane verzije kliknite gumb Live Update na vrhu prvog ekrana da biste ručno preuzeli datoteke. Drugi AV softverski paketi imaju slične mehanizme za automatsko ažuriranje.

Ako vašem AV softveru nije dostupno automatsko ažuriranje (što je malo vjerojatno), tada bi trebao imati barem jasne upute kako se pristupa njegovoj Web lokaciji za preuzimanje ažuriranih verzija.

Možete se zaštiti od *malwarea* redovitim ažuriranjem ostalog softvera, posebno operativnog sustava i aplikacija kao što je Internet Explorer. U 7. poglavlju nalaze se detaljne informacije o tome kako se ovaj softver ažurira.

4.5 Što učiniti ako imate virus ili crva

Postoje velike šanse, čak i ako održavate svoju obranu, da vaše računalo jednom bude zaraženo. Ali zaraza nije uzrok za paničarenje. Možete se oporaviti, ponekad vrlo jednostavno, od napada virusa ili crva.

Kako vidjeti je li računalo zaraženo?

Najbolji način provjere je li računalo zaraženo jest pokretanje redovitog AV skeniranja korištenjem najnovijih potpisa. Vaše se računalo može skenirati i preko Interneta. Na primjer, Symantec Security Check skenira vaše računalo preko Interneta u potrazi za virusima i ostalim *malwareom*. Da biste pokrenuli besplatno skeniranje prijeđite na adresu www.symantec.com/avcenter/index.html i kliknite ikonu Check for Security Risks pri dnu stranice.

Slične besplatne usluge nude i drugi AV proizvođači. Na lokaciji www.mcafee.com, kliknite Home pa vezu Home Office i potražite okvir Free Tools s lijeve strane prve stranice koja se otvorila. Na adresi www.trendmicro.com kliknite vezu Personal. Vidjet ćete vezu Trend Micro House Call pri vrhu stranice. Ta veza pokreće besplatno skeniranje virusa. Panda Software pruža besplatan alat za skeniranje na adresi http://www.pandasoftware.com/activescan/com/activescan_principal.htm.

Međutim, skeniranje možda neće otkriti novi *malware* koji nema potpis. Zato pratite izdajničke znakove koji mogu upućivati na zarazu. Na primjer, jesu li datoteke oštećene ili nedostaju, ili jesu li promijenjene postavke neke aplikacije te je li onemogućen softver za zaštitu? Je li vaše računalo odjednom postalo usporeno ili se čudno ponaša? Je li vaš vatrozid otkrio programe koje niste otvarali a koji pokušavaju uspostaviti vezu s Internetom? Sve ovo su znakovi koji upućuju na to da možda imate problema.

Kako ukloniti virus ili crva?

Kada na svojm računalu otkrijete virus, trebate pokrenuti svoj AV softver da ga on ukloni. Kada je skeniranje dovršeno, softver bi vas trebao upozoriti da uklonite ili izolirate svaki virus koji je otkrio. (Izolirati *malware* znači ostaviti ga na računalu, ali u nekom izoliranom stanju u kojem ne može napraviti nikakvu štetu.) AV softver također može očistiti datoteke koje su zaražene virusom.

Proizvođač vašeg AV softvera ponudit će i posebne alate za uklanjanje crva i *malwarea* kao što su trojanski konji (o kojima detaljno govorimo u 5. poglavlju). Te alate možete preuzeti s Web lokacije AV proizvođača. Vaš bi AV trebao moći preporučiti jesu li vam potrebni dodatni alati. U okviru na kraju ovog poglavlja "Uklanjanje varijante crva Beagle" provest ću vas kroz korake koje sam ja poduzeo da uklonim crva koji je pronašao put do mojeg računala.

U najgorem slučaju AV softver neće moći ukloniti *malware*. Ako se to dogodi, možda ćete trebati pomoć izvana. Kontaktirajte službu podrške korisnicima svojeg AV proizvođača da biste doznali što vam oni preporučuju (ali se pripremite na dugo čekanje). Možete kontaktirati i proizvođača svojeg računala, potražiti pomoć u trgovini u kojoj ste računalo kupili (uz naknadu, naravno) ili kontaktirati lokalni servis za popravak računala za pomoć.

Posljednja mogućnost je da počnete od nule i jednostavno reinstalirate operativni sustav i aplikacije s originalnih diskova sa softverom. Da biste to učinili, jednostavno umetnite originalni disk operativnog sustava u CD-ROM pogon i uključite računalo. Računalo će tražiti da ponovno potvrdite želju za reinstaliranjem operativnog sustava. Međutim, reinstaliranje operativnog sustava briše sve podatke koje ste spremili na svoje računalo (nadajmo se da imate dobre navike kreiranja sigurnosnih kopija). Svakako se uvjerite da ste iscrpili sve opcije prije početka ponovnog formatiranja svojeg tvrdog diska.

4.6 Kako odabrati neki antivirusni proizvod?

Ako već nemate neki antivirusni proizvod, na raspolaganju imate nevjerojatan izbor. Tri najveća proizvođača su Symantec, koji prodaje Norton AntiVirus; Trend Micro, koji prodaje PC-cillin; i McAfee, koji prodaje VirusScan.

Prednosti odabira rješenja jednog od velike trojke je u tome što oni imaju dobro utemeljene istraživačke timove koji proizvode potpise za nove viruse u kratkom roku od njihova pojavljivanja i imaju infrastrukturu za distribuiranje ažuriranih verzija svojoj bazi klijenata. Loša je strana ovih rješenja najviša cijena.

Vrlo blizu velike trojke su razne kompanije koje također nude vrlo dobre proizvode. To su Computer Associates, Kaspersky Lab, F-Secure, ZoneLabs, ESET i Panda Software.

Organizacija GriSoft nudi i besplatan antivirusni softver. Njezin proizvod AVG Anti-Virus sadrži sve uobičajene značajke proizvoda koji se plaćaju. On skenira nove datoteke i programe i e-poštu i omogućuje vam da provodite skeniranja

cijelog tvrdog diska. Softver nudi i specijalizirani alat za uklanjanje virusa te sadrži automatska ažuriranja potpisa za nove viruse. Jedina mana je ta što korisnici besplatne verzije ne dobivaju nikakvu tehničku podršku. Ako ste registrirani korisnik, svoja pitanja može poslati stručnim korisnicima AVG-a na *online* forumu, ali ne možete poslati poruku e-pošte ili razgovarati s osobom iz odjela za tehničku podršku ako niste nabavili plaćenu verziju. (No, čak i rješenje koje se plaća jeftinije je od većine AV proizvoda.)

Općenito se sa sigurnošću može reći da svi ovi proizvodi pružaju istu razinu sigurnosti. Većina kompanija nudi besplatni probni rok da biste mogli ispitati razne programe. Ispitivanje nekoliko programa je pametno, jer vam daje priliku da vidite koji od tih programa ima korisničko sučelje i *online* dokumentaciju koje vam najviše odgovaraju. U tablici 4.3 nalazi se popis AV proizvođača, Web lokacija na kojima možete dobiti besplatne probne verzije ili kupiti proizvod. Sredinom 2005. godine cijene su se kretale u rasponu od 24,95 do 49,95 američkih dolara za samostalan antivirusni softver, iako specijalne ponude i rabati mogu utjecati na krajnju cijenu. Kao što je već prije spomenuto, dobit ćete veću vrijednost od proizvoda koji uključuje druge funkcije zaštite uz zaštitu od virusa.

Ako tražite više savjeta, časopisi i Web lokacije kao što su *PC Magazine* (www.pcmagazine.com), *PC World* (www.pcworld.com) i CNET (www.cnet.com) redovito daju recenzije korisničkih sigurnosnih proizvoda i često objavljuju "izbor

Tablica 4.3

Vodeći antivirusni proizvodi

Proizvod	Proizvođač	Web lokacija
Anti-Virus Personal	Kaspersky Lab	www.kaspersky.com
AVG Anti-Virus	GriSoft	http://free.grisoft.com
eTrust Antivirus	Computer Associates	www.ca.com
F-Secure Anti-Virus	F-Secure	www.f-secure.com
NOD32	ESET	www.eset.com
Norton AntiVirus	Symantec	www.symantec.com
PC-cillin	Trend Micro	www.trendmicro.com
Titanium Antivirus	Panda Software	www.pandasoftware.com
VirusScan	McAfee	www.mcafee.com
ZoneAlarm AntiVirus	Zone Labs	www.zonelabs.com

urednika". Recenzije možete pročitati da biste usporedili cijene i značajke na ovim lokacijama.

4.7 Popis za provjeru

Upotrijebite ovaj popis za provjeru kao brzi referentni vodič za materijal iznesen u ovom poglavlju.

Učinite

- Upotrijebite antivirusni softver, bilo samostalan ili kao dio rješenja u paketu.
- Redovito provodite skeniranje svojeg računala i ažurirajte svoj antivirusni softver.
- Redovito ažurirajte svoj operativni sustav i softver pretraživača.
- Redovito kreirajte sigurnosne kopije važnih datoteka.

Nemojte učiniti

- Nemojte otvarati sumnjive ili netražene poruke e-pošte od pošiljatelja koje ne poznajete.
- Nemojte klikati veze unutar poruka e-pošte ili otvarati priloge koje su poslali vama nepoznati ljudi.

4.8 Korisni izvori

Ovaj odjeljak predstavlja dodatne izvore koji vam mogu pomoći da više naučite.

Svi AV proizvođači u ovom poglavlju uključuju informacije o pojavama virusa, najnovijim AV ažuriranjima i alatima za uklanjanje *malwarea*. Oni također pružaju savjete za izbjegavanje infekcije *malwareom* i za zaštitu PC-a.

Virus List na adresi www.viruslist.com, koju vodi AV proizvođač Kaspersky Lab, odličan je izvor informacija o *malwareu*, *spamu*, zlonamjernim napadačima i općenito o problemima sigurnosti Interneta. Lokacija obuhvaća enciklopediju tema o *malwareu* i savjete koji će vam pomoći da vaše računalo bude sigurnije.

Virus Bulletin na adresi www.virusbtn.com sadrži gomilu informacija o virusima i *malwareu*. Na njemu se prodaje i bilten s informacijama antivirusne istraživačke zajednice.

WildList Organization na adresi www.wildlist.org sebe smatra mjerodavnom za provjeru proizvođača antivirusnog softvera, što može napuhati tvrdnje o broju postojećih virusa. Za ovo postoji razlog. Ovisno o tome od kojeg AV proizvođača koristite brojeve virusa, broj virusa kreće se negdje između 50 000 i 90 000 i stalno raste. Međutim, broj virusa koji se brzo šire znatno je manji.

Ova organizacija prati viruse za koje se smatra da štete običnim korisnicima računala u njihovom svakodnevnom radu. Virusi 'u divljini' stavljeni su nasuprot virusa koje su u laboratoriju otkrili istraživači ili su izdani kao dokazi koncepta, bez stvarnog širenja. WildList se oslanja na volontere iz antivirusne istraživačke zajednice i druge ljude da bi dala svoj doprinos uzorcima virusa i pratila viruse 'u divljini'.

Uklanjanje varijante crva Beagle

Pred kraj siječnja 2005. godine moje je kućno računalo zarazila varijanta crva Beagle pod nazivom Beagle.BA. (Većina AV proizvoda naziva je crv Beagle.) Varijanta je nova verzija prethodno izdanog komada *malwarea.* Varijante nastaju kada pisci *malwarea* uzmu neki postojeći crv ili virus, te ga izmijene ili postave dodatak softveru. Beagle.BA je *mass-mailer* crv koji također pokušava isključiti antivirusni i sigurnosni softver koji se izvodi na stroju-domaćinu. Ovo nije neuobičajena tehnika za crve, naročito one koji nastoje umetnuti trojanske konje na računalo kako bi kasnije napadač mogao koristiti stroj. Sreća za mene, Beagle.BA nije u svojem *payloadu* donio trojanskog konja.

Shvatio sam da sam zaražen kada je regularno skeniranje tvrdog diska otkrilo crva. Norton AntiVirus izbrisao je crva s mojeg računala, ali je i preporučio preuzimanje posebnog alata za popravak kako bi se popravila svaka šteta koju je crv mogao uzrokovati prilikom instaliranja na moje računalo.

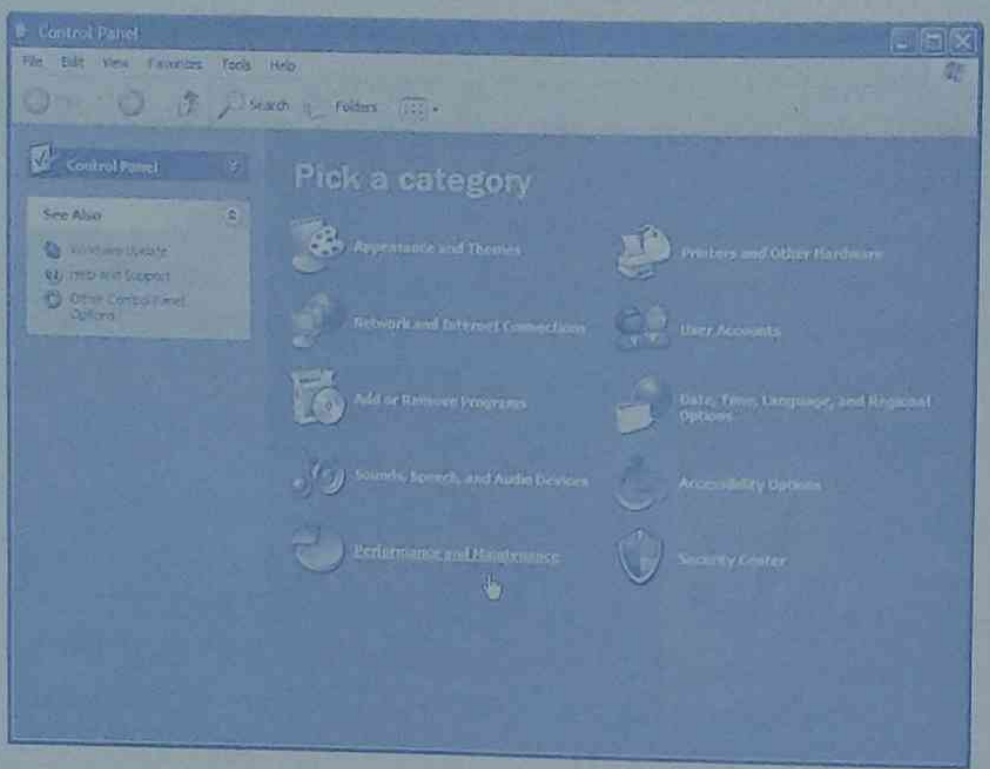
Odsurfao sam do lokacije www.symantec.com i kliknuo vezu Security Response koja me odvela na početnu stranicu Security Response. U to je vrijeme varijanta Beagle.BA i dalje bila popisana na prvoj stranici Security Responsea, pa sam kliknuo vezu koja me odvela direktno do alata za uklanjanje varijante Beagle.BA. (Ako ne možete pronaći određeni virus na popisu na prvoj stranici Security Responsea, njegovo ime možete upisati u polje za pretraživanje da biste pronašli pravu stranicu.)

nastavlja se...

Upute na Web stranici preporučile su mi da isključim System Restore. System Restore je funkcija u sustavu Windows koja nadzire promjene osnovnih datoteka sustava i registryja koje omogućuju funkcioniranje operativnog sustava. Funkciju System Restore možete koristiti da napravite brzu snimku poznatog, dobrog stanja kada vaše računalo ispravno radi. Ako je nešto pokvarilo ispravan rad, možete upotrijebiti System Restore da vratite poznato dobro stanje.

No, *malware* se često sprema u datoteke sustava i registryje, pa je moguće da je System Restore spremio crva ili virus i ponovno instalirao *malware* na vaše računalo. Onemogućavanjem funkcije System Restore, uklanjate sve prethodne točke obnavljanja koje su tamo pohranjene. Da biste doznali više o funkciji System Restore, kliknite Start, zatim kliknite gumb Help and Support i u polje za pretraživanje upišite System Restore overview.

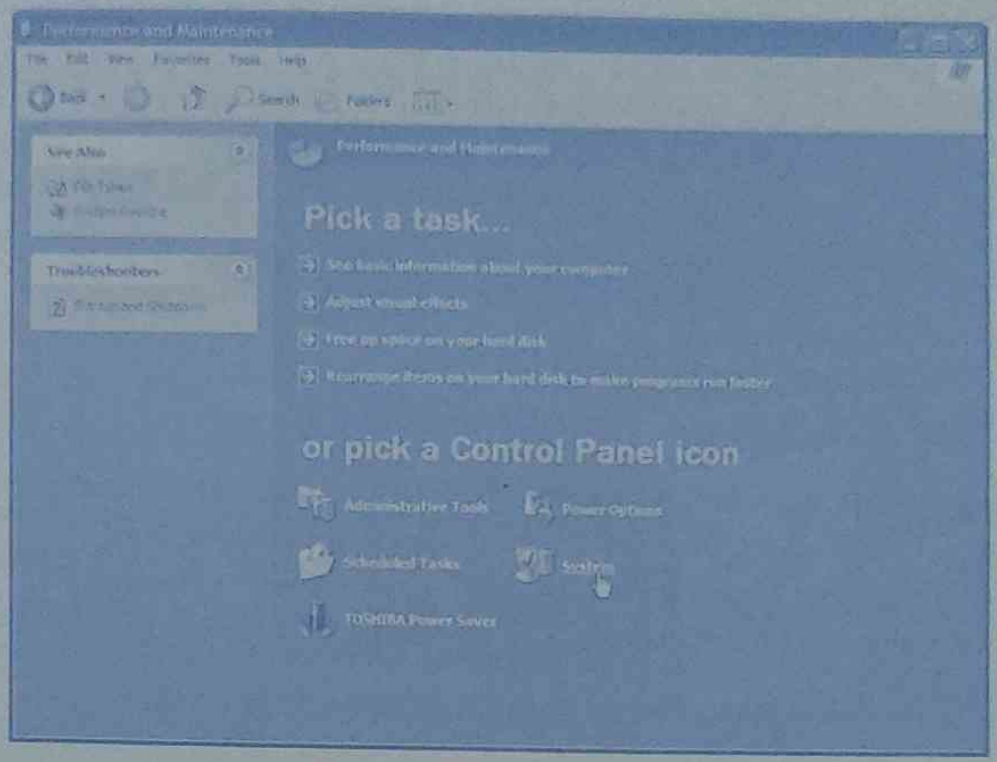
Privremeno onemogućavanje funkcije System Restore ne utječe na vaše osobne datoteke kao što su dokumenti Worda, slike i mediji. Da biste onemogućili System Restore, kliknite Start pa odaberite Control Panel. (Ovisno o tome kako ste postavili svoj izbornik Start možda ćete morati



Slika 4.1 Kategorija Performance and Maintenance u Control Panelu

kliknuti Settings da pronađete opciju Control Panel.) Kada kliknete otvara se prozor u kojem piše Pick a category (odaberi kategoriju, op. prev.) kao što je prikazano na slici 4.4.

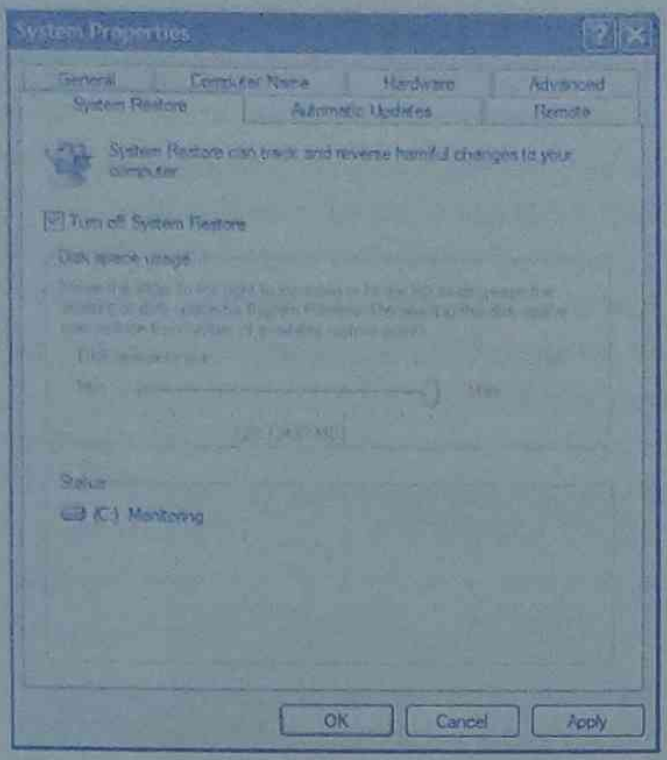
Odaberite kategoriju Performance and Maintenance pa kliknite opciju System kao što je prikazano na slici 4.5. Pojavljuje se manji prozor System Properties (slika 4.6). Taj prozor ima nekoliko kartica kao što su General, Computer Name i Hardware. Odaberite jahač System Restore i vidjet ćete potvrdni okvir označen s Turn off System Restore. Potvrdite taj okvir i kliknite gumb Apply na dnu prozora.



Slika 4.2 Kategorija System u Performance and Maintenance

Nakon što sam to napravio, preuzeo sam alat, koji se zove FxBeagle i pokrenuo ga na svojem računalu. Kada je alat završio, vratio sam se u prozor System Restore i ponovno uključio funkciju System Restore. Nakon toga sam proveo skeniranje cijelog diska još jedanput da se uvjerim je li računalo čisto.

nastavlja se...



Slika 4.3 Dijaloški okvir System Properties.

Ako ste sigurni da je vaše računalo čisto, možete sami postaviti vlastitu točku obnavljanja. Da biste postavili točku obnavljanja kliknite Start i odaberite All Programs, Accessories, System Tools i System Restore. Čarobnjak će vas provesti kroz korake koji su potrebni za postavljanje točaka obnavljanja.

5. poglavlje

Kako se riješiti nepoželjnih gostiju? 2. dio: *spyware, adware* i trojanski konji

U prethodnom smo poglavlju raspravljali o porastu *malwarea* i istražili dvije posebne vrste *malwarea*: viruse i crve. U ovom poglavlju ispitujemo tri druge raspoznatljive vrste sigurnosnih rizika: *spyware, adware* i trojanske konje. Neko ćemo vrijeme utrošiti na definiranje svakog od ovih rizika, pogledati koji su pravni i tehnološki problemi sa *spywareom* i *adwareom* i objasniti kako se možete zaštititi od tih prijetnji.

5.1 Što su *spyware, adware* i trojanski konji?

U užem smislu, *spyware* je pojam za neke tehnologije uhođenja (naročito, izvršne aplikacije) koje se provode na vašem računalu bez primjerenog upozorenja, vaše suglasnosti ili kontrole. *Spyware* može nadzirati vaše *online* aktivnosti i/ili provoditi funkcije bez vašeg znanja ili pristanka. Ovisno o programu, *spyware* može pratiti i izvještavati o svakoj Web lokaciji koju posjetite, generirati iskočne oglase, promijeniti polaznu stranicu i postavke pretraživača ili bilježiti svaku tipku koju pritisnete. U širem smislu, *spyware* se često koristi kao općeniti naziv za većinu

vrsta potencijalno nepoželjnih tehnologija koje otkrivaju antivirusni programi. Ove se tehnologije implementiraju na načine koji vam onemogućuju upravljanje skupljanjem, korištenjem i distribucijom osobnih informacija; uzrokuju materijalne promjene koje utječu na rad računala, privatnost i sigurnost; i povrh toga koriste vaš sustav kao resurs. To su stavke o kojima korisnici *anti-spyware* softvera trebaju biti obaviješteni i koje moraju lako moći ukloniti ili onemogućiti.

Adware je podskup šire kategorije *spywarea*, koji je dizajniran da isporučuje ciljano oglašavanje na vaš Web pretraživač, naročito preko iskočnih oglasa. *Adware* je često upakiran s drugim softverskim programima, kao što su programi za razmjenu datoteka, igre ili drugi pomoćni programi koji se mogu besplatno preuzeti s Weba. *Adware* zna koje vam vrste oglasa treba isporučiti jer prati koja mjesta na Internetu posjećujete. Na primjer, ako surfate po nekoj lokaciji za iznajmljivanje automobila, *adware* program može generirati iskočni oglas koji je naručila konkurentska tvrtka za iznajmljivanje automobila. Osim praćenja vašeg *surfanja* i dosađivanja s oglasima, *adware* može i otvoriti vezu s Internetom da bi na središnji poslužitelj slao izvještaje o vašim navikama *surfanja*. Te informacije, koje mogu obuhvaćati vašu dob, spol, navike kupovanja pa čak i vašu lokaciju, mogu se koristiti za "istraživanje tržišta" za privlačenje novih klijenata.

Trojanski konji su programi koji se predstavljaju da su netko drugi. Na primjer, trojanski konj može se oglašavati kao zabavni animirani isječak, čuvar ekrana ili besplatan softverski program koji obećaje da će napraviti nešto "super" ili nešto korisno. Ali trojanski konji također uključuju neobjavljene funkcije (ako, zapravo, obećana funkcija uopće radi). Najčešći cilj trojanskog konja je da instalira stražnja vrata na vašem računalu ili ukrade lozinke. Stražnja vrata omogućuju napadačima udaljenu kontrolu nad vašim strojem. Neke klase *spywarea* mogu se smatrati i trojanskim konjima jer dolaze uz lažno predstavljanje. Na primjer, mogli biste s Interneta preuzeti zgodan mali čuvar ekrana s krasnim leptirima koji također nadzire vaše navike surfanja po Webu ili bilježi pritiske na tipke. Trojanski konji često se oslanjaju na viruse, crve i društveni inženjering da bi potaknuli korisnike koji ništa ne sumnjaju da ih preuzmu s Interneta.

Pojam *trojanski konj* postao je skraćeni naziv svakog programa koji se nalazi na vašem računalu i osigurava udaljeni pristup neovlaštenoj osobi ili provodi nepoželjne funkcije. Većina antivirusnih programa i neki *anti-spyware* programi mogu otkriti trojanske konje.

Spyware, *adware* i trojanski konji ne mogu sami sebe replicirati. Zato ove kategorije aplikacija trebaju načine za širenje. Trojanski konji mogu se, primjerice, isporučiti kao *payload* crva ili virusa, uključiti u poruku e-pošte kao prilog ili upakirati s drugim softverom. *Spyware* i *adware* koriste slične tehnike širenja, ali se oni

najčešće preuzimaju kao dio "besplatnog" programa za dijeljenje datoteka ili pomoćnog softvera, ili tehnikom pokretanja po učitavanju (prilikom čega vi posjetite neku Web lokaciju koja instalira program bez vaše dozvole).

Definiranje *spywarea* i *adwarea*

Dok se sigurnosni rizici, poput *spywarea* i *adwarea* mogu smatrati proširenjima problema virusa, postoje značajne razlike u načinu na koji su ti programi prosuđeni kao poželjni i nepoželjni i želite li ih na svojim strojevima. Virusi, crvi i trojanski konji uvijek su nepoželjni i treba ih se automatski ukloniti s računala. Mnoge vrste programa klasificirane kao *adware* i *spyware* također su visokorizične i mogu imati značajan negativni utjecaj na rad računala ili mogu ugroziti vašu privatnost prijenosom vaših osobnih informacija trećoj strani.

No, ostali *adware* programi niskog su rizika. Oni mogu isporučiti korisnu funkcionalnost poput igara ili pomoćnih programa i imaju razmjerno mali utjecaj na privatnost i rad računala. Kao što je emitiranje televizijskih programa besplatno jer televizijske kuće zarađuju na oglašavanju, mnogi softverski programi također su besplatni za preuzimanje jer se i oni oslanjaju na oglašavanje da bi ostvarili prihod. Takvi se softverski programi nazivaju programi podržani oglašavanjem *(ad-supported programs)*. Oni uključuju *adware* za isporuku ciljanih oglasa. Neki softverski programi podržani oglašavanjem traže dopuštenje korisnika prije nego što instaliraju *adware*, a ostali ne. No, ostali rade u sivom području u kojem je dopuštenje korisnika dio ugovora o licenci softvera napisan sitnim slovima. Istražit ćemo ove razlike i što one znače u sljedećim odjeljcima.

Široki raspon *spyware* i *adware* ili potencijalno nepoželjnih programa može se podijeliti u dvije glavne kategorije: visokorizični zlonamjerni programi i niskorizični programi. Istraživači sigurnosti stavljaju *spyware* i *adware* programe u jednu od ovih kategorija ovisno o tome kako se programi instaliraju, koje podatke pokušavaju izvesti s vašeg računala, kakav utjecaj imaju na rad računala i što znate o njihovom radu i namjeri. Kada istraživači ispituju ponašanje programa da bi odredili visinu rizika, zapravo ispituju brojna ključna područja, uključujući karakteristike instalacije, svojstva prikrivenog rada, utjecaj na privatnost, utjecaj na integritet, utjecaj na performanse i jednostavnost uklanjanja:

- Utječe li program na stabilnost sustava i usporava li vezu s mrežom?
- Lansira li program iskočne oglase? Ako da, koliko često?
- Služi li program kao sredstvo za preuzimanje i instaliranje drugih rizika za sigurnost (kao što su dodatni *spyware* i/ili *adware*)?
- Je li program izmijenio polaznu stranicu pretraživača ili promijenio odrednice za pretraživanje ili ponašanje?

- Je li program uzrokovao otkrivanje povjerljivih, osjetljivih informacija kao što su računi u bankama i lozinke?
- Je li program otkrio manje osjetljive podatke kao što je praćenje vaših navika surfanja Webom?
- Ima li program politiku za zaštitu privatnosti, i odgovara li njegovo ponašanje toj politici?
- Pokušava li se program sakriti ili izbjeći da ga instalira korisnik, uključujući nepoželjno ponovno instaliranje i tehnike za ponovno pokretanje procesa koje je prekinuo korisnik?
- Nedostaje li programu značajka za deinstaliranje ili se nije registrirao u području Microsoft Windowsa Add or Remove Programs?
- Instalira li se program potiho, uz malo ili bez ikakvih naznaka korisniku?
- Nedostaje li programu korisničko sučelje?
- Prikriva li program svoje procese ili ih skriva od korisnika s nekim nejasnim imenom?
- Je li korisnik obaviješten o prisutnosti programa samo preko ugovora o licenci za krajnjeg korisnika *(End User License Agreement – EULA)*? Djeluje li kao da se EULA odnosi na neki drugi program?

Da bi se kvalificirali kao visokorizični ili zlonamjerni *spyware* i *adware*, programi moraju imati značajan utjecaj na stabilnost i/ili performanse sustava ili moraju objavljivati povjerljive, osjetljive informacije i/ili dokazivati skriveno ponašanje poput tihe instalacije, nedostatka korisničkog sučelja i zatajivanja rada aplikacija. Primjeri visokorizičnih programa mogu obuhvaćati *keystroke loggere*, otimače pretraživača i *dialere*. (Tablica 5.1 opisuje ove i druge vrste programa.) Zlonamjerni *spyware* je ilegalan i koriste ga kriminalci koji žele krasti od vas. On se instalira na vaše računalo kroz 'pukotine' u softveru, preko crva i virusa, društvenog inženjeringa i pokretanjem po učitavanju.

Programi niskog rizika uključuju mnoge popularne komercijalne ili oglasima potpomognute oglase i provode neželjene funkcije, poput mijenjanja polazne stranice, usmjeravanja na nepoznate tražilice ili instaliranja alatnih traka u vaš Web pretraživač koje niste tražili i koje ne želite. *Adware* može čitati i kolačiće instalirane na vaše računalo da bi otkrio informacije o vašim Web navikama.

Naravno, bez obzira na stupanj rizika programa, vi, korisnik, trebali biste imati potpunu kontrolu nad programima na svojem računalu, uključujući mogućnost pronalaženja i uklanjanja svih programa koje ne želite. Kao što ćete vidjeti u sljedećem odjeljku, neki *spyware* i *adware* programi pokušavaju preoteti tu kontrolu.

Tablica 5.1

Definicije Spywarea

Pojam	Definicija
Spyware	*Spyware* je općenita klasa softverskih programa koji nadziru aktivnosti računala i prenose te informacije na druga računala ili lokacije na Internetu. Među informacijama koje se mogu aktivno ili pasivno pokupiti i prenijeti *spywareom* su lozinke, detalji prijava za rad, brojevi računa, osobne informacije, pojedinačne datoteke i osobni dokumenti. *Spyware* može pokupiti i distribuirati informacije koje se odnose na računalo korisnika, aplikacije koje se na njemu izvode, korištenje Internet pretraživača i druge računalne navike. *Spyware* se učitava na računalo korisnika uglavnom bez znanja korisnika, a kreiraju ga napadači iz podzemlja ili kriminalci.
Adware	*Adware* je vrsta tehnologije prikazivanja oglasa – radi se uglavnom o izvršivim aplikacijama čija je primarna svrha isporuka sadržaja oglasa. Mnoge *adware* aplikacije provode i praćenje funkcija pa se zato mogu kategorizirati kao tehnologije za praćenje. Korisnici će vjerojatno željeti ukloniti *adware* ako primijete takvo praćenje; ne žele gledati oglase koji takav program generira ili ih frustrira njegov učinak na performanse sustava. Neki korisnici će možda htjeti zadržati određeni dio *adware* programa ako je njihova prisutnost uvjet za drugi besplatan softver. *Adware* kreiraju komercijalne softverske tvrtke, a ne kriminalci i često je upakiran s popularnim besplatnim softverom, kao što su programi za dijeljenje datoteka. Neki *adware* programi opisuju svoje funkcije u ugovoru o licenci i pružaju opcije za deinstaliranje; drugi se pak mogu instalirati na računalo bez dopuštenja korisnika i spriječiti pokušaj korisnika da ih ukloni.
Keystroke logger (poznat i kao *keylogger*)	*Keyloggeri* su tehnologije za praćenje koji nedopušteno bilježe aktivnosti na tipkovnici. *Keyloggeri* tipično pohranjuju zabilježene pritiske na tipke za kasnije učitavanje ili ih prenose na udaljeni procesor ili osobi koja koristi *keylogger* preko e-pošte. *Keystroke loggeri* se koriste za krađu lozinki i druge informacije o identitetu.
Browser hijacker (otimači pretraživača)	*Browser hijackeri* nanovo umeću polaznu stranicu i preusmjeravaju vaš pretraživač na neželjene ili nepoznate tražilice ili druge Web lokacije. Neki *browser hijackeri* mogu vas spriječiti prilikom objavljanja polazne stranice. Neki rade tako da brišu unos za polaznu stranicu koju ste odabrali i umeću vlastitu u posebnu datoteku koju konzultira vaše računalo (*hosts* datoteka). Oni također mogu presresti unose za pretraživanje upisane u legitimnu tražilicu i prikazati vlastite rezultate.

nastavlja se...

Definicije Spywarea *(nastavak)*	
Pojam	**Definicija**
Browser Helper Object (BHO)	BHO-i su popratne aplikacije za Microsoft Internet Explorer (IE) koje se automatski izvode svaki put kada pokrenete IE. Oni su isto oblik alata za upravljanje stanjem. Mnoge su tehnologije za praćenje ili za prikazivanje oglasa implementirane kao BHO-i. BHO-i mogu pronaći Web stranice koje korisnik posjećuje i zamijeniti banner oglase koje generira Web poslužitelj ciljanim oglasima. BHO-i mogu i nadzirati i izvještavati korisnikovo surfersko ponašanje te ponovno umetnuti polaznu stranicu korisnika. Zamijetite da svi BHO-i nisu zlonamjerni; mnoge su alatne trake legitimnih Web pretraživača BHO-i.
Trojanski konji	Trojanski konji su softverske krabulje bezazlenih ili korisnih programa koje zavaravaju korisnike da ih instaliraju na svoja računala. Kada su instalirani, trojanski konji provode nepoželjne ili neobjavljene funkcije.
Remote Access/Administration Tool (RAT)	RAT-ovi (*rat* je štakor na engleskom jeziku, op. prev.) su izvršive aplikacije dizajniranje da omoguće udaljeni pristup ili kontrolnu sustava. Oni su vrsta tehnologije upravljanja na daljinu. Mnoge legitimne upotrebe RAT-ova ne predstavljaju prijetnju za sigurnost, ali se mogu zlonamjerno upotrijebiti, naročito ako ih koristi netko tko nije legitimni vlasnik računala ili administrator.
Dialer	*Dialeri* su programi koji koriste modem računala za pozivanje ili pristupanje uslugama. Korisnici žele ukloniti *dialere* jer biraju neočekivane telefonske brojeve i nabijaju velike telefonske račune. *Dialer* je kolokvijalan izraz za tehnologije biranja telefonskih brojeva.

5.2 Tehnički i zakonski izazovi otkrivanja i uklanjanja *spywarea* i *adwarea*

4. poglavlje, "Kako se riješiti nepoželjnih gostiju, 1. dio: virusi i crvi" opisivalo je nekoliko razloga porasta *malwarea* (jednostavnost komunikacije, homogeno računalno okruženje, reaktivni sigurnosni softver). Ti se faktori svakako odnose i na porast *spywarea*, ali nedvojbeni *raison d'être* (razlog postojanja) *spywarea* i *adwarea* je novac. Bilo da se krade identitet, regrutira računalo u bot mrežu za iznajmljivanje ili se generira prihod od oglašavanja sumnjivih softverskih tvrtki, na ovu vrstu aplikacije uvelike utječe znak dolara. Potencijalni profiti koji se mogu generirati čine problem *spywarea/adwarea* mnogo težim za rješavanje. *Spyware*

brokeri mogu zaposliti programere da kontinuirano preuređuju kôd da bi se bolje izbjegavalo otkrivanje i uklanjanje preko sigurnosnog softvera ili potaklo razvoj programa otvorenog koda i stručnih biblioteka.

Koliko je ovaj posao profitabilan? Razmotrite ovo: jedna *adware* tvrtka pod nazivom Claria zaradila je približno 90 milijuna američkih dolara u 2003. godini. (*Adware* proizvodi tvrtke Claria poznati su kao GAIN ili Gator i često se isporučuju u paketu sa softverom treće strane kao što je Kazaa, softver za izravnu razmjenu datoteka.) Uz profite poput ovoga, *adware* tvrtke imaju snažnu motivaciju da nastave sa svojim radom. Druge *adware* tvrtke uključuju WhenU., 180Solutions, Avenue Media i Direct Revenue.

Brojni pokazatelji demonstriraju proširenost *spywarea* i *adwarea*. ISP, Earthlink, proveo je studiju s WebRootom, koji proizvodi *anti-spyware* softver. Skenirali su više od 3,2 milijuna PC-a i pronašli u prosjeku 26 *spyware* programa po računalu. Dell Computer tvrdi da su problemi *spywarea* primarni uzrok poziva službi za tehničku podršku. Symantec je proveo studiju da ustanovi koje su kategorije Web lokacija iza sebe ostavljale najnepoželjniji softver. Istraživači su uzeli potpuno novi PC, povezali ga s Internetom bez ikakve standardne softverske zaštite i pretraživali. Testeri su radili jedan sat i svaki je provodio interakciju s različitim kategorijama Web lokacija. Iznenađujuće, dječje Web lokacije istovarile su najviše nepoželjnog softvera na računalo – 359 komada *adwarea* u samo jednom satu surfanja. Usporedbom, drugi najveći broj bio je 64 komada *adwarea* instaliranog s lokacija za organiziranje putovanja. Kockarske lokacije istovarile su najviše *spywarea*, četiri komada. Tablica 5.2 sadrži puni popis rezultata.

Tablica 5.2

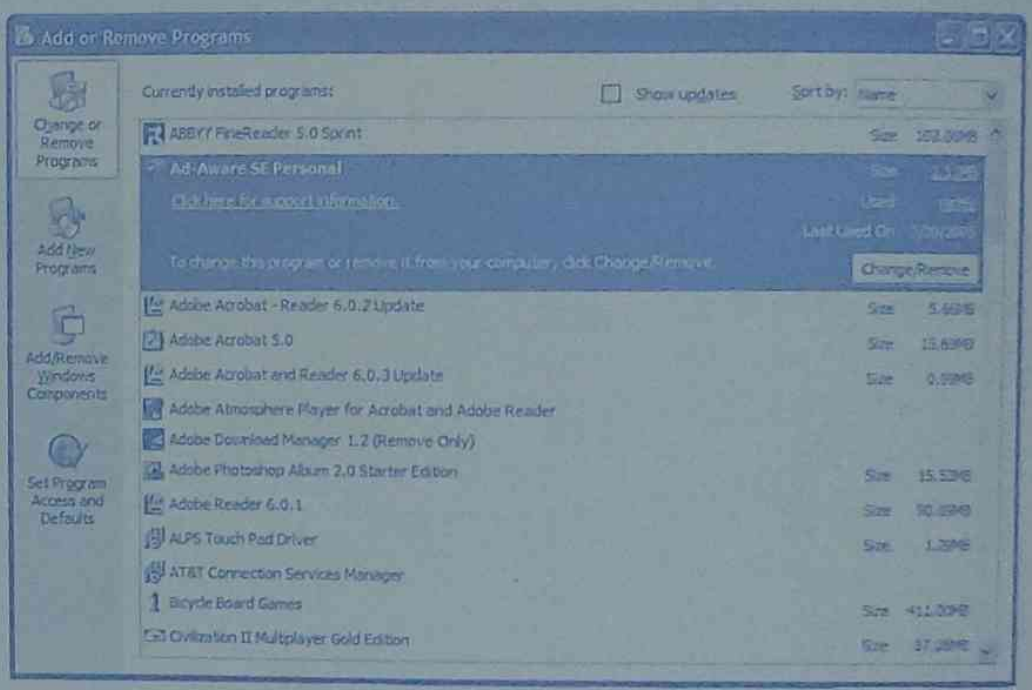
Symantecova studija

Kategorija lokacije	Adware	Spyware	Otimači	Kolačići
Kockanje	23	4	2	68
Djeca	359	0	3	31
Novosti	3	1	0	26
Maloprodaja	2	1	1	22
Kupovina	0	0	0	10
Sportovi	17	2	0	72
Putovanja	64	2	1	35

Kreatori visokorizičnih *adwarea* i *spywarea* nastoje da se njihov softver teško pronalazi i uklanja. Na primjer, *spyware* program može na neko računalo postaviti tisuće datoteka i provesti tisuće izmjena u Registryju. Kao što je napomenuto u 4. poglavlju, Registry je baza podataka konfiguracijskih postavki koje govore računalu o aplikacijama i korisničkim profilima na vašem stroju. Vaše se računalo obraća Registryju prilikom pokretanja i svaki put kada otvarate programe. *Spyware* i *adware* često umeću sebe u Registry da postanu jedni od programa koje računalo automatski izvodi.

Spyware i *adware* mogu postaviti dvije vlastite kopije na računalo, pa ako jednu izbrišete, izvodit će se dalje sigurnosna kopija. Ili mogu posijati "*tricklere*" (nešto što kapa, op. prev.) na vaše računalo. *Trickleri* su sićušni komadi softvera koji preuzimaju nepoželjne programe ponovno nakon što su ti programi bili obrisani ili deinstalirani.

Legitimni softver je relativno lako deinstalirati pomoću funkcije Add or Remove Programs u sustavu Windows XP, prikazane na slici 5.1. U osnovi ta funkcija popisuje sve programe na vašem računalu i pruža vam opciju da svaki od programa pojedinačno deinstalirate. Jedan od indikatora visokorizičnih *adware* ili *spyware* programa je taj da se oni ne nalaze na tom popisu programa. Da biste vidjeli popis programa na svojem računalu, kliknite gumb Start pa odaberite Add/Remove. Ako se stavka Add/Remove ne nalazi na vašem izborniku Start, odaberite Control Panel, a zatim Add or Remove Programs. Legitimni *adware* program pojavit će se u ovom području i omogućiti vam da ga uklonite.



Slika 5.1 Add or Remove Programs

Neki *spyware* programi idu toliko daleko da se instaliraju bez vašeg dopuštenja (na primjer, čak i ako kliknete "No, I don't want this program", one će se ipak instalirati) ili bez vašeg znanja (pokretanje po učitavanju). Sve ove karakteristike čine *spyware* i *adware* teške za otkriti i ukloniti.

Neke *adware* tvrtke tvrde da namjeravaju postati bolji Internet građani. Na primjer, Claria i WhenU. tvrde kako su se odrekle prljavih trikova kao što je pokretanje po učitavanju da bi instalirale svoj softver na računala korisnika. (No, neki istraživači prigovaraju da one i dalje korisnicima otežavaju pronalazak i deinstaliranje njihovih programa.)

Drugi proizvođači *adwarea* ne opterećuju se pojavom legitimnosti i nastavljaju prljavo igrati, čak i jedni s drugima. Na primjer, u 2004. godini Avenue Media optužila je tvrtku DirectRevenue zbog kreiranja softvera za pronalaženje i uklanjanje *adwarea* tvrtke Avenue Media da bi instalirala vlastiti na računala korisnika.

Osim tehničkih problema zaštite i uklanjanja *spywarea* i *adwarea*, postoje i zakonski problemi koji se trebaju riješiti. Iako su neke kategorije *spywarea* nezakonite (kao što su *keystroke loggeri*), *adware* uživa kvazi-legalni status. Na primjer, svaki *adware* koji obavještava korisnika o svojoj funkciji u EULA-i, je, uglavnom legalan. To je zbog toga što ste vi, korisnik, navodno pročitali i složili se s uvjetima sadržanim u EULA-u. Prije nego što počne preuzimanje, morate kliknuti gumb na kojem piše nešto poput "I agree to the terms and conditions set forth in this license". Klik tog gumba isto je što i potpisivanje fizičkog ugovora; kada jednom kliknete Yes, slažete se sa svime što je rečeno u EULA-i. Međutim, skoro nitko ne čita EULA-e, a to *adware* tvrtke znaju. (Za detaljne informacije pročitajte okvir na kraju ovog poglavlja "Čitanje teksta napisanog sitnim slovima".)

Preporučljivo je da potražite i pročitate EULA za svaku lokaciju koju posjećujete ili programe koje preuzimate. Ako program nema EULA-u ili pokušava sakriti svoju namjeru iza nerazumljivog jezika, uzmite to kao znak upozorenja i razmislite o tome da program ne preuzmete.

Međutim, jedno o pitanja u raspravi koja se odnosi na *adware* EULA-e je određivanje toga od čega se zapravo sastoji zadovoljavajuća obavijest i pristanak. Ako neki *adware* program zapravo opisuje svoju funkciju u EULA-i, smatra li se to zadovoljavajućom obavijesti? Što ako je opis zakopan unutar dugačkog ugovora te je nerazumljivo iznesen?

Nedavno su predložena brojna federalna zakonodavna rješenja kako bi se riješio problem *spywarea* i *adwarea*, uključujući i pitanje zadovoljavajuće obavijesti i pristanka. Od 1. lipnja 2005. godine uvedena su dva prijedloga zakona u Kongresu i Senatu. U Donjem domu kongresa, donošenje zakona poznatog kao SPY ACT (Securely Protect Yourself Against Computer Trespassers, H.R. 29) sponzorirala je kongresmenka Mary Bono. SPY ACT bi općenito neprihvatljivo ponašanje, kao što je instaliranje softvera bez vašeg dopuštenja, proglasio nezakonitim. Ovaj prijedlog zakona također određuje da isporučitelji *adwarea* moraju jasno navesti funkciju softvera, vrstu informacija koje sakupljaju i namjenu tog skupljanja informacija. On također određuje da *adware* mora korisniku pružiti mogućnost da odbije njegovo instaliranje ili da ga ukloniti u bilo kojem trenutku bez "pretjeranog napora". Drugi prijedlog zakona Kongresa, I-SPY Prevention Act of 2005 (H.R. 744), uveo je 10. veljače 2005. godine kongresmen Bob Goodlatte. Taj se prijedlog zakona fokusira u velikoj mjeri na poduzimanje prinudnih akcija i naplaćivanje kazni zločestim dečkima. Ovaj prijedlog dodaje novi Section 1030A u Criminal Code pod nazivom "Illicit indirect use of protected computers" i tvori tri kriminalne zabrane.

U Senatu je zakon SPY BLOCK Act (S. 687) uveo senator Conrad Burns sa senatorima Ronom Wydenom i Barbarom Boxer 20. ožujka 2005. godine. Zakon brani instaliranje softvera na nečije računalo bez prethodne obavijesti i pristanka i zahtijeva razumne procedure za deinstaliranje svih softverskih programa koji se mogu preuzimati s Interneta. Zakon Enhanced Consumer Protection Against Spyware Act of 2005, koji je uveo senator Allen sa senatorima Smithom Ensignom 11. svibnja 2005. godine, dopuštao bi zapljenu profita tvrtkama i pojedincima koji su potajno instalirali *spyware* na računala. Taj bi zakon tražio znatno više prekršajne i krivične kazne za one koji trguju ili sudjeluju na neki drugi način u trgovini *spywareom*. Taj bi zakon također prisilio Federalnu trgovinsku komisiju da tuži *spywareske* provale.

Sva četiri prijedloga zakona prepoznaju da se mnoge tehnologije koje se koriste u zlonamjerne i prijevarne svrhe mogu također koristiti i u korisne i zakonske svrhe. Prema zakonu, *adware* i *spyware* ne moraju nužno tehnologiju činiti lošom ili nezakonitom. Ovi prijedlozi zakona samo traže da se regulira zlorabljenje *adwarea* i *spywarea*.

1.lipnja 2005. godine su H.R. 29 i H.R. 744 proslijeđeni Donjem domu kongresa. Preostaje da Senat provede glasovanje za svoja dva prijedloga zakona, te da se Donji dom kongresa i Senat slože u kombiniranju prijedloga zakona koji bi prošao u oba doma. I na kraju, predsjednik bi trebao usvojiti prijedlog zakona.

Sva četiri prijedloga možete pročitati odlaskom na Thomas, stranicu za pretraživanje koju vodi Library of Congress za pronalaženje zakona *online*. Prijeđite na adresu http://thomas.loc.gov i upišite naziv prijedloga zakona ili broj u polje za traženje 109th Congress.

Uz federalne zakonodavne aktivnosti ove godine, usvojeno je više od 40 prijedloga zakona koji se odnose na *spyware*.

Federalna trgovinska komisija također je raspravljala o problemu *spywarea*. U ožujku 2005. godine komisija je objavila izvještaj pod nazivom "Nadziranje softvera na vašem računalu: *spyware*, *adware* i ostali softver". Izvještaj ističe probleme koji su pridruženi definiranju *spywarea*, rizike koje *spyware* predstavlja za korisnike i načine na koje bi vlada i vodeće kompanije u industriji trebali odgovoriti na problem *spywarea*. Da biste pronašli kopiju izvještaja pročitajte odjeljak "Korisni izvori" na kraju ovog poglavlja.

Zakonski problemi kompliciraju i trud proizvođača *anti-spyware* programa kako da se nose sa *adwareom*. 2003 godine Claria je tužila PC PitStop, *anti-spyware* organizaciju, zbog klevete. PC PitStop je nazvala proizvode tvrtke Claria *spywareom* što kompanija nije smatrala točnim. 2005. godine proizvođači popularnog softvera WeatherBug žalili su se kada je Microsoftov *anti-spyware* proizvod popisao jednu oglašivačku komponentu unutar WeatherBuga kao rizik za privatnost. Microsoft je pregledao žalbu i uklonio potpis koji je otkrivao oglašivački poslužitelj.

Neki *anti-spyware* proizvodi dolaze u sukob s ostalim proizvodima drugih odjela unutar iste tvrtke. Portal Yahoo! nudi besplatan *anti-spyware* program na svojoj alatnoj traci Yahoo!. Ali kad je proizvod prvi put lansiran, tražio je od korisnika da posebno zahtijevaju skeniranje zbog *adwarea* uz *spyware*. Razlog tome je što je divizija Yahoo!-a, Overture, koja nudi plaćene popise pretraživanja, poslovni partner Claria Corporationa. Prema priči iz lipnja 2004. godine u eWeeku[1], Overture je dao plaćene popise SearchScoutu, usluzi Claria koja prikazuje "pop-under" oglašavanje. (Ti se oglasi prikazuju ispod stranice; vidite ih nakon što zatvorite pretraživač.) SearchScout je bila zaslužna za 31 posto prihoda tvrtke Claria u 2003. godini. Yahoo! je od tada promijenio svoju *anti-spyware* alatnu traku da uz *spyware* traži i *adware*.

Jedan od načina na koji *anti-spyware* tvrtke mogu izbjeći problem je usvajanje diplomatičnijeg jezika. Na primjer, McAfeeov *anti-spyware* softver koristi pojam

---

1 "Yahoo Plays Favorites with Some Adware", Matt Hicks, objavljeno 1. lipnja 2004. godine u eWeeku (www.eweek.com).

"Potentially Unwanted Programs" (potencijalno nepoželjni programi) umjesto pojmova 'adware' ili 'spyware'. Microsoftov *anti-spyware* softver oblači rukavice i naziva sve "Potentially Unwanted Software". (Pretvorite li ovo u kraticu, dobit ćete PUS (gnoj, op. prev.). Ne znam jesu li to dečki iz Microsofta odabrali namjerno, ali to prikazuje osjećaje ljudi koji su imali posla s ovom vrstom problema. Ovo je također kraće od mojeg vlastitog izraza, koji se isto može pretvoriti u kraticu: Bad, Annoying Software That All of us Require be Deleted Speedily.)

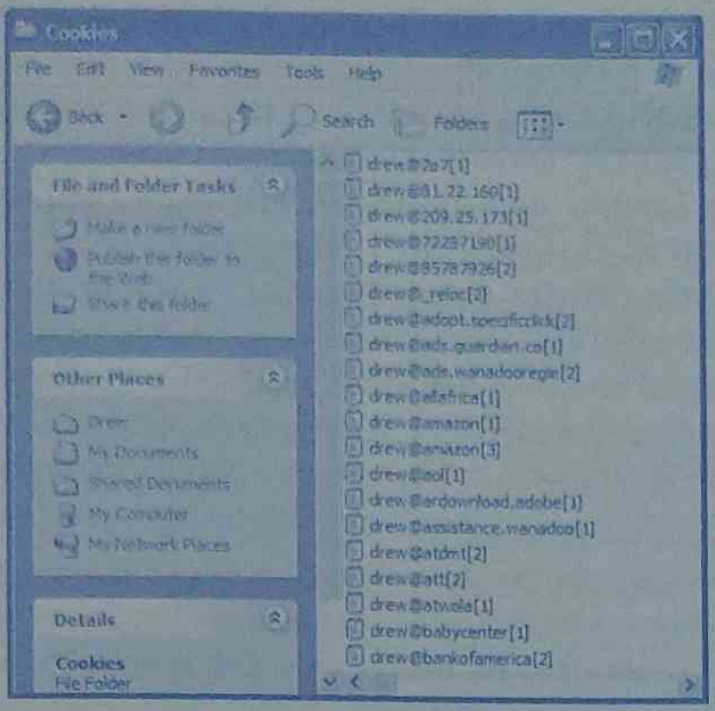
Želite li kolačić?

Kolačići (cookies) predstavljaju još jednu poteškoću pri klasificiranju i rješavanju problema s provalničkim i nepoželjnim programima. Kolačići su male tekstualne datoteke koje Web pretraživač postavlja na vaše računalo kada posjetite neku Web lokaciju. Kolačići sadrže informacije o vama, kao što su vaše korisničke preference ili informacije o prijavi za rad. Svaki put kada se vratite na tu Web lokaciju, odgovarajući se kolačić prenosi s vašeg računala na Web lokaciju da bi pomogao u prilagođavanju vašeg posjeta. Na primjer, ako ste redoviti klijent neke lokacije za e-trgovinu, ta lokacija može pohraniti informacije o vama u kolačiću na vašem računalu, kao što je povijest kupovanja, omiljeni artikli itd. Kolačići koriste iskustvo e-trgovanja i općenito su bezopasni.

Međutim, druga kategorija kolačića, koja se naziva kolačić za praćenje (tracking cookie), bilježi informacije o drugim Web lokacijama koje posjećujete i dijelite te informacije s ostalim lokacijama. Oglačivačke mreže skupljaju te informacije za provođenje istraživanja tržišta i koriste ih kao pomoć pri slanju ciljanih oglasa na vaše računalo. Dobar *anti-spyware* softver trebao bi otkriti kolačiće za praćenje i dati vam opciju da ih izbrišete.

Kolačiće na svojem računalu možete vidjeti ako odete u mapu My Computer. Kliknite mapu Local Disk (C:), zatim Documents and Settings, tada svoje korisničko ime, a potom mapu Cookies. Međutim, pregledavanjem kolačića nećete saznati mnogo o tome radi li se o standardnim kolačićima ili o kolačićima za praćenje. Većina kolačića sastoji se od mnogo brojeva koji imaju značenje za neki Web poslužitelj, ali ne i za ljudsko biće. Međutim, pregledavanjem popisa Cookies moći ćete vidjeti koje Web lokacije postavljaju kolačiće na vaš tvrdi disk. Možete ih izbrisati tako da istaknete određenu datoteku i kliknete naredbu Delete this file na lijevoj strani prozora, kao što se vidi na slici 5.2.

Podešavanjem postavki privatnosti u svojem Web pretraživaču možete odrediti kako Web lokacije mogu polagati kolačiće na vaše računalo i mogu li to uopće

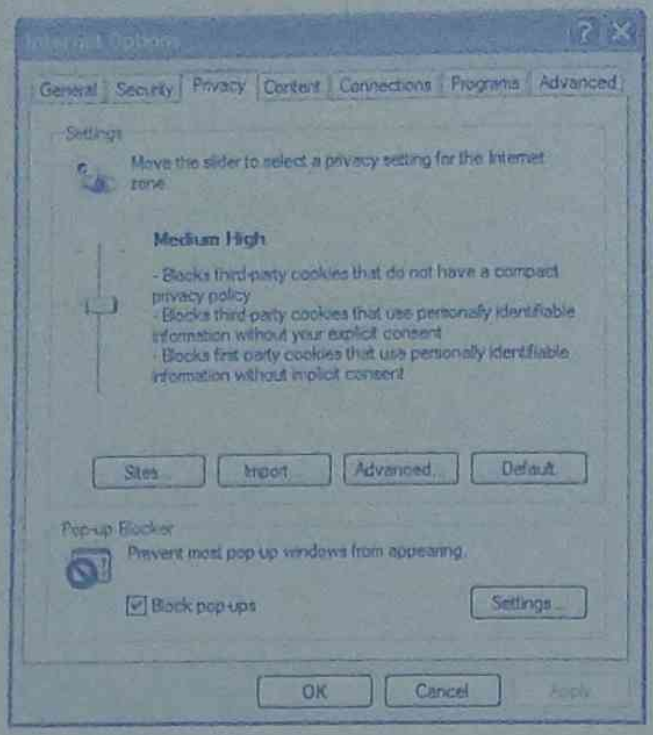


Slika 5.2 Brisanje kolačića

činiti. Ako koristite Internet Explorer, otvorite pretraživač i odaberite Tools, Internet Options, Privacy. Klizač na traci podešava postavku privatnosti i govori Web pretraživaču koje vrste kolačića prihvaća, kao što je prikazano na slici 5.3. Opcije su u rasponu od prihvaćanja svih kolačića do blokiranja svih kolačića s gradacijama između ovih dviju krajnosti. Microsoftova osnovna postavka je Medium High, što znači da će vaš pretraživač blokirati svaki kolačić koji pokuša upotrijebiti informacije otkrivanja identiteta bez vašeg eksplicitnog pristanka.

Zapamtite, nisu svi kolačići invazivni. Na primjer, ako izbrišete kolačiće neke lokacije za e-trgovinu koju redovito koristite, možda ćete otkriti da je prilagodba u kojoj ste uživali izbrisana. Isto tako, postavljanje zaštite od kolačića na previsoku razinu, može blokirati korištenje nekih lokacija. Na primjer Yahoo! Web račun e-pošte neće raditi s postavkom sigurnosti Block All Cookies ili High u Internet Exploreru. Postavka Cookie detaljno je objašnjena u 7. poglavlju "Sigurnost Windowsa".

Drugi primjer ovakvog objekta za praćenje su Local Shared Objecti (LSO-ovi), koje je najbolje smatrati programskim kolačićima Macromedia Flasha. Neka Web lokacija može koristiti LSO za spremanje informacija na vaše računalo kao što su



Slika 5.3 Postavljanje opcija za kolačiće u IE-u

najbolji rezultat neke igre ili podataci koje ste upisali. Za razliku od kolačića, LSO-ove ne možete onemogućiti preko normalnih postavki pretraživača.

5.3 Kako *spyware/adware* i trojanski konji inficiraju vaše računalo

Spyware, *adware* i trojanski konji mogu na vaš stroj dospjeti na brojne načine – putem Web pretraživača, e-pošte ili u paketu s drugim softverom koji ste preuzeli s Interneta. Poznavajući način na koji je taj softver dospio na vaš stroj, imat ćete bolju ideju kako ga izbjeći.

Iz Web pretraživača

Jedan od razloga popularnosti Web pretraživača kao mehanizma transporta *spywarea* i *adwarea* je ActiveX. ActiveX je Microsoft tehnologija dizajnirana da omogući korisnicima ulaganje interaktivnih objekata, često multimedije, na Web stranice. ActiveX pomaže kreiranje interaktivnijih Web stranica, kroz primjerice, animaciju ili sposobnosti otvaranja drugih aplikacija u pretraživaču (poput Microsoft Worda ili Adobea). Osim oživljavanja Web stranica, ActiveX tehnologija može na vašem računalu i izvršavati programe koji se nazivaju ActiveX kontrole,

preko Web pretraživača Internet Explorera. ActiveX kontrole provode interakciju s operativnim sustavom kao i svaki drugi izvršivi softver. ActiveX programi isporučuju se s digitalnim potpisima autora programa (odnosno, tvrtke koja je program kreirala, a ne osobe koja je razvila softver). Digitalne potpise smatrajte osobnim potpisima na papiru. Vaš pretraživač može potražiti digitalni potpis i vidjeti je li on originalan da biste vi bili sigurni tko je program potpisao. Imate dva izbora: prihvatiti program i dopustiti mu da radi što god želi na vašem računalu ili ga odbiti. ActiveX sigurnost oslanja se na vašu ispravnu odluku o tome koje programe prihvatiti. Neke ActiveX kontrole su bezopasne i unaprjeđuju doživljaj *surfanja*, ali pisci *malwarea* mogu također kreirati ActiveX kontrole da bi instalirali nepoželjne programe na vaše računalo. Ako prihvatite zlonamjerni program, uvalit ćete se u veliku nevolju.

Svoj pretraživač Internet Explorer možete podesiti tako da vas obavijesti kada se neka ActiveX kontrola učita na vaše računalo. Da biste saznali kako se to radi, pročitajte odjeljak "Podesite postavke svojeg pretraživača".

Pisci *spywarea* i *malwarea* mogu iskoristiti i ranjivosti softvera u pretraživačima (uključujući i alternativne pretraživače kao što je Mozilla Firefox). Svaki softverski proizvod na svijetu ima mane koje otkrivaju istraživači. Neki od tih istraživača su stručnjaci za pitanja sigurnosti; ostali su zlonamjerni napadači koji koriste svoje pronalaske da bi napadali ranjivi softver. Budući da je Internet Explorer najrasprostranjeniji pretraživač, on je i najpopularnija meta napadača. Na primjer, u lipnju 2004. godine pojavio se trojanski konj pod nazivom Download.ject. Koristeći se pukotinama u IE-u i u IIS-u (Internet Information Server, što je Windows softver za Web poslužitelje), taj se trojanski konj instalirao na računala korisnika ako su oni samo posjetili neku Web stranicu s zaraženog Web poslužitelja. Download.ject je primjer programa čije se instaliranje pokreće po učitavanju. Napadi koji koriste pukotine u softveru najbolje se rješavaju primjenom ispravki softvera koje se nazivaju zakrpe (patches), a koje kreiraju i distribuiraju proizvođači softvera. Na primjer, svakog drugog utorka u mjesecu Microsoft objavljuje najnoviju rundu zakrpa za svoj softver. Da biste te zakrpe preuzeli, posjetite stranicu http://windowsupdate.microsoft.com.

Iz drugog softvera

Najkorištenija metoda širenja *adwarea* je da se on uključi u paket s drugim programima, kao što je softver za dijeljenje datoteka ili za zabavu te zgodni pomoćni programčići. Ponekad vas isporučitelj softvera koji želite upozorava na *adware* koji će se također instalirati, a ponekad upozorenja nema. U većini slučajeva, softver koji želite, kao što je program za dijeljenje datoteka ne radi ako onemogućite

adware koji se s tim softverom isporučuje. (Pročitajte okvir "Čitanje teksta napisanog sitnim slovima" na kraju poglavlja.)

Iz e-pošte

Spyware i trojanski konji mogu na vaše računalo stići u porukama e-pošte kao prilozi. Na primjer, mnogi *phishing* napadi, u kojima *scam artist* koristi e-poštu da bi prijevarom od vas dobio lozinke, matične brojeve i druge osjetljive informacije, uključuju i *malware* kao što su *keystroke loggeri*.

Iz društvenog inženjeringa

Kao što smo objasnili u 2. poglavlju "Sprječavanje krađe identiteta", društveni inženjering je ljepše ime za 'laž'. *Spyware* i *adware* snabdjevači nisu iznad toga da vam slažu kako bi vas namamili da instalirate softver. Većina uobičajenih primjera društvenog inženjeringa svodi se na oglašavanje nekog programa ili priloga u poruci e-pošte kao nečega što to nije. Odličan primjer je crv Naked Wife koji se pojavio 2001. godine. On se širio porukama e-pošte koje su sadržavale prilog "sa zločestim Flash filmom". Prilog je zapravo bio trojanski konj koji se instalirao na vaše računalo, te se slao e-poštom svim primateljima iz vašeg adresara, nakon čega bi počeo brisati datoteke.

5.4 Kako se zaštiti od *spywarea, adwarea* i trojanskih konja?

Svoje računalo možete zaštiti od zaraze *spywareom, adwareom* i trojanskim konjima na različite načine. Ovaj odjeljak ističe nekoliko metoda.

Koristite *anti-spyware* i antivirusni softver

Najbolji način zaštite od *spywarea* i trojanskih konja je korištenje *anti-spyware* i antivirusnog softvera. Obje vrste softvera mogu spriječiti instaliranje poznatih *spywarea* i trojanskih konja na vaše računalo, te mogu spriječiti i instaliranje nepoznatog *malwarea*.

Mnogi proizvođači antivirusnih programa sada nude i zaštitu od *spywarea* i *adwarea* kao dio većeg programskog paketa koji uključuje antivirusni program i vatrozid. Ti paketi su odlična opcija jer je s njima lakše raditi nego s pregrštom samostalnih programa. Isto tako, ne trebate brinuti o tome hoće li proizvod A uzrokovati nepravilan rad proizvoda B (ili hoće li proizvodi A i B uzrokovati nepravilan rad računala).

Uz već rečeno, možda ćete ipak željeti dodatnu zaštitu koju pruža samostalan *anti-spyware* softver. Zašto? Najjednostavniji razlog je strategija dubinske obrane (poznata i kao pristup pojas-i-naramenice); jedan proizvod može uloviti *spyware* ili *adware* koji je drugi proizvod propustio.

Pa zašto onda ne biste imali dva različita antivirusna programa? Činjenica je da mnoge korporacije koriste baš ovu strategiju: poslužitelji za e-poštu napune se antivirusnim softverom od AV tvrtke 1, dok korporativna računala dobiju antivirusni softver tvrtke 2. Međutim, korisnici zaista ne trebaju dva antivirusna proizvoda jer, općenito govoreći, AV proizvođači utemeljili su paritetnost – svaki AV isporučitelj zna posao jednako dobro kao i ostali.

To nije nužno tako kada se radi o *spywareu* i *adwareu*. Tvrtke koje kreiraju sigurnosni softver i dalje se muče prilikom definiranja što su zapravo *spyware* i *adware*. Svaka tvrtka ima svoj vlastiti skup definicija, što znači da svaka kompanija identificira i rješava *spyware* i *adware* na malo drugačiji način. Povrh svega, pisci *spywarea* i *adwarea* dokazali su se lukavima i inovativnima, te stalno pronalaze nove načine ukapanja u vaša računala. Novi *spyware* i *adware* programi pojavljuju se nevjerojatnom brzinom, pa jedna tvrtka može imati potpise za njih prije neke druge tvrtke, ili jedna tvrtka može razviti alat za njihovo uklanjanje brže od druge tvrtke. Rezultat je da *anti-spyware* zaštita tvrtke A može biti u nekim područjima bolja ali u drugima lošija i obratno, od tvrtke B.

Možete kupiti samostalan *anti-spyware* softver od različitih proizvođača, a na raspolaganju su vam i dobre besplatne opcije. Zato čak i ako vaš AV softver već skenira tražeći *spyware*, možda ćete htjeti još jedanput provjeriti s nekim drugim *anti-spyware* alatom. Tablice 5.3 i 5.4 sadrže popise vodećih *anti-spyware* softvera, i to verzija koje se plaćaju i onih besplatnih.

Ako izvodite dva odvojena *anti-spyware* programa, nemojte se začuditi ako oni počnu stvarati probleme. Ako se to dogodi, morat ćete se odlučiti za samo jedan program, a drugi odbaciti.

Vrhunska imena na *anti-spyware* tržištu uključuju Sunbelt Software, koji proizvodi CounterSpy; Webroot Softwar, koji proizvodi Spy Sweeper; Lavasoft, koji proizvodi Ad-Aware; Tenebril, koji proizvodi SpyCatche; i Computer Associates, koji prodaje eTrust PestPatrol. Etablirani proizvođači antivirusnih rješenja također prodaju *anti-spyware* alate, a manji proizvođači također nude dobre proizvode. Tablica 5.3 sadrži popis tih proizvođača. Od sredine 2005. godine cijene se kreću u rasponu od 19,95 do 29,95 američkih dolara za samostalne *anti-spyware* programe i od 49,95 do 69,95 dolara za zaštitne programske pakete koji uključuju *anti-spyware*, antivirusne programe, vatrozid i druge sigurnosne proizvode. Imajte na umu da posebne ponude i rabati mogu utjecati na krajnju cijenu.

Tablica 5.3

Komercijalni anti-spyware proizvodi		
Proizvod	**Proizvođač**	**Web lokacija**
ActiveScan Pro	Panda Software	www.pandasoftware.com
Ad-Aware SE Plus	Lavasoft	www.lavasoft.com
CounterSpy	Sunbelt Software	www.sunbeltsoftware.com
eTrust PestPatrol	Computer Associates	www.ca.com
F-Secure Anti-Spyware for Windows	F-Secure	www.f-secure.com
McAfee Antispyware	McAfee	www.mcafee.com
PC-cillin	Trend Micro	www.trendmicro.com
SpyCatcher	Tenebril	www.tenebril.com
Spy Sweeper	Webroot Software	www.webroot.com
Spyware Eliminator	Aluria Software	www.aluriasoftware.com
Symantec Norton Internet Security Spyware Edition	Symantec	www.symantec.com

Pri odabiru proizvoda potražite sustav koji vam omogućuje provođenje redovitog skeniranja i otkrivanja potencijalnog *spywarea* u realnom vremenu. Potražite proizvode koji mogu otkriti i ukloniti *spyware* i izolirati sumnjive programe. (Funkcija karantene ili izoliranja sprječava izvršavanje programa, ali ga ne uklanja. Izoliranje vam dopušta da istražite trebate li program ukloniti.)

Poput proizvoda vatrozidova i AV proizvoda, *anti-spyware* proizvodi traže da odlučite što učiniti s programom koji su otkrili. Ponekad je odluka laka, ali u nekim slučajevima nećete biti sigurni. *Anti-spyware* programi često vam pružaju informacije o programima koje su otkrili, ali one mogu biti toliko tehničke da vam neće pomoći. Zato potražite programe koji pružaju razumljive informacije koje će vam pomoći da donesete odluku.

Softver morate i stalno ažurirati. Potražite sučelje koje ažuriranje čini jednostavnim – ili, još bolje, automatizira proces ažuriranja. Iskoristite besplatne probne rokove za testiranje sučelja, da biste pronašli ono koje će vam biti najkorisnije.

U donošenju odluke koji proizvod izabrati, provjerite recenzije iz *PC Magazinea* (www.pcmagazine.com), *PC Worlda* (www.pcworld.com) i CNET-a (www.cnet.com) te iz domaćih časopisa kao što su VIDI (www.vidi.hr), PC Chipa (www.pcchip.hr) BUG-a (www.bug.hr) i ostalih informatičkih časopisa na hrvatskom tržištu, koji

redovito pišu recenzije i ocjenjuju sigurnosne proizvode. Mogli biste provjeriti i *online* forume za preporuke i recenzije. Ako znate engleski, dobri su forumi dostupni na (www.castlecops.com) i SpywareInfo (www.spywareinfo.com).

Pazite na oportuniste

Antivirusni proizvodi postoje godinama. U tom su razdoblju inferiorni i nerazumljivi programi nestali, dok je u isto vrijeme respektabilna grupa tvrtki razvila stabilne proizvode koji uglavnom rade kako su i oglašeni. *Anti-spyware* tržište je u svojem razvoju, a tržišne sile koje režu slabe i tvrtke bez reputacije tek trebaju uzeti maha. Mnogi su proizvodi dojurili na tržište i ne rade baš jako dobro. Neki proizvodi pokušavaju i zbuniti korisnike uzimajući nazive slične nazivima popularnih *anti-spyware* softvera ili registriranjem sličnih Web lokacija. Na primjer, popularni alat za sprječavanje otmice pretraživača pod nazivom HijackThis često koriste imitatori ili isporučitelji *malwarea* u nadi da će na svoje lokacije privući korisnike koji ništa ne sumnjaju. Pravi alat HijackThis dostupan je na adresi www.merijn.org/downloads.html.

Dodatno, mogućnosti koje pruža vruć novi tehnološki sektor privlači i one koji ne koriste bezazlene i (legalne) taktike da vas uvjere da kupite njihov softver. Na primjer, u ožujku 2005. godine FTC je uložila tužbu protiv proizvoda pod nazivom Spyware Assassin. Prema izjavi FTC-a, Spyware Assassin nudi varljivo besplatno skeniranje za otkrivanje *spyware* na računalima korisnika, čak i kada *spyware* ne postoji. Ta je prijevara otišla toliko daleko da je popisala imena i lokacije datoteka *spyware* na čistim računalima. Spyware Assassin je potom ponudio *anti-spyware* softver (za 29.95 USD) koji, kako tvrdi FTC čak ni ne radi tako dobro.

Niste li baš zbog zahtjeva za skeniranjem posjetili neku lokaciju, budite sumnjičavi ako nepozvani i alarmirajući iskočni okviri traže da kliknete ili da odmah pokrenete skeniranje – ili ako tvrde da je otkriven *spyware* na vašem računalu, a da vi niste ni zatražili skeniranje. Kao i u stvarnom svijetu, čuvajte se tih taktika prodaje koje su vrlo agresivne.

Proizvođači popisani u ovom poglavlju imaju reputaciju i s njima možete bez bojazni poslovati. Ako neki proizvođač nije na popisu, to ne znači da njegov proizvod nije dobar. Odnosno, ako radite s novom ili malo poznatom tvrtkom, budite oprezni. Na primjer, tvrtke s reputacijom jasno objavljuju EULA-e i odrednice za osiguranje privatnosti na svojim Web lokacijama. Jedan od načina na koji možete provjeriti neku tvrtku je potražiti njezino ime i vidjeti kakve ćete rezultate dobiti. Ime te tvrtke možete poslati i na neki *anti-spyware* forum da biste dobili informacije o reputaciji tvrtke ili da biste saznali imaju li drugi pozitivna ili negativna iskustva s tom tvrtkom.

Besplatan *anti-spyware* softver

Najbolja stvar u vezi s besplatnim *anti-spyware* softverom je ta da je besplatan! Ako ne želite platiti za *anti-spyware* softver, ove su tri opcije apsolutno preporučljive. Možete ih koristiti kao pričuvnu verziju plaćenog softvera da biste osigurali da je vaš sustav koliko je to moguće čist (ili da biste provjerili radi li plaćeni softver dobar posao. Zamijetite da, ako koristite nekoliko *anti-spyware* alata, jedan može popisati drugog kao *spyware*. Na primjer, mnogi *anti-spyware* programi popisuju Spybot Search&Destroy, besplatan *anti-spyware* program, kao *spyware*.

Mana besplatnog softvera je ta da možete izgubiti na drugim prednostima, kao što je tehnička podrška korisnicima. Uz to, neke besplatne *anti-spyware* programe piše i održava jedna osoba ili mala grupa dobrovoljaca, što znači da bi oni mogli biti sporiji u izdavanju novih potpisa, novih značajki i ispravki softvera komercijalnih proizvođača. Možda ćete trebati potražiti i ručno preuzimati nove ažurirane verzije, dok se komercijalni proizvodi uglavnom automatski ažuriraju.

Dva najpopularnija besplatna *anti-spyware* proizvoda su Lavasoftova. Lavasoft prodaje i komercijalnu verziju Ad-Aware, ali Spybot je besplatan (iako njegovom kreatoru možete dati donacije, ako vam se alat svidi). Lavasoft i Spybot Search&Destroy imaju forume na koje možete slati svoja pitanja i pronaći nove informacije o softveru.

U siječnju 2005.godine Microsoft je izdao besplatan *anti-spyware* alat pod, lukavim nazivom Microsoft AntiSpyware. Potporni program kupljen je od tvrtke GIANT Software Company. Softver uključuje skeniranje i preventivno blokiranje. Možete sudjelovati u SpyNet zajednici, forumu za skupljanje i objavljivanje informacija o nepoželjnom softveru.

Drugi dobro poznati alat je *anti-spyware* skener ugrađen u Yahoo! alatnu traku. Otkrivanje *spywarea* tek je jedna njegova značajka; druge obuhvaćaju blokiranje iskočnih oglasa i veza na druge Yahoo! lokacije. Ako preuzmete ovu alatnu traku dobit ćete pristup *anti-spyware* zajednici i moći ćete pisati poruke na oglasnu ploču i primati informacije o novim prijetnjama *spywarea*. Zamijetite da se *anti-spyware* skener na Yahoo! alatnoj traci temelji na softveru eTrust PestPatrol tvrtke Computer Associates

Možete također preuzeti dva korisna besplatna alata – HijackThis i CWShredder. HijackThis daje dnevnik vašeg Registryja koji možete upotrijebiti da biste otkrili nepoželjne programe kao što su otimači pretraživača. CWShredder je alat za uklanjanje CoolWebSearch *adwarea*, koji je iz obitelji nekih od najvirulentnijih i najupornijih *malware* na Internetu. InterMute, tvrtku koja nudi CWShredder za besplatno preuzimanje, kupila je tvrtka Trend Micro. U vrijeme pisanja ovog

poglavlja mogli ste još uvijek pronaći CWShredder na adresi www.intermute.com/products/cwshredder.html. To vjerojatno neće ostati tako. Možda ćete trebati pretražiti lokaciju www.trendmicro.com za ovaj softver ili ga preuzeti s Web lokacije Merijna Bellekom, koji je stvorio CWShredder (i HijackThis). Tablica 5.4 sadrži popis svih Web lokacija koje nude besplatan softver.

Što može *anti-spyware* softver?

Anti-spyware proizvodi mogu skenirati vaš tvrdi disk i pronaći nepoželjni softver. Kada otkriju taj softver pitaju vas želite li ga izbrisati, izolirati ili ga ostaviti gdje je. (Izoliranjem *spyware* ostavljate ga na svojem računalu, ali sprječavate njegovo funkcioniranje.) Mnogi proizvodi provode i proaktivni nadzor da bi osigurali sprječavanje instaliranja nepoželjnog softvera na vaš stroj. Na primjer, Microsoft AntiSpyware uključuje komponente koje nadziru postavke vaših aplikacija i računalnog sustava u realnom vremenu. On vas upozorava kada se pokušavaju promijeniti aplikacije ili postavke. Također nadzire programe na vašem računalu u pokušaju pristupanja Internetu.

Poput AV softvera o kojem smo govorili u 4. poglavlju, *anti-spyware* softver koristi potpise da bi otkrio *malware* na vašem računalu. Anti-spyware skenira

Tablica 5.4

Besplatan anti-spyware softver

Proizvod	Proizvođač	Web lokacija
Ad-Aware SE Persona	Lavasoft	www.lavasoft.com
HijackThis i CWShredder*	Merijn/InterMute	www.merijn.org/downloads.html (za HijackThis i CWShredder) http://www.intermute.com/products/cwshredder.html (za CWShredder)
Microsoft AntiSpyware	Microsoft	www.microsoft.com
Spybot Search&Destroy	Safer-Networking	www.safer-networking.org
Yahoo! Toolbar with Anti-Spy	Yahoo!	http://toolbar.yahoo.com/ie

* *HijackThis and CWShredder nisu potpuna anti-spyware rješenja. HijackThis je alat za ručno uklanjanje otimača pretraživača. CWShredder je alat za uklanjanje jedino za CoolWebSearch, koji je izbacio cijelu obitelj varijanti spywarea. Zamijetite i da su Web lokacije za Merijn, Lavasoft i Spybot ponekad žrtve DoS napada ili drugih pokušaja rušenja. Ako vam te lokacije budu nedostupne, pokušajte ih kasnije ponovno posjetiti.*

datoteke, registryje i programe na vašem tvrdom disku tražeći otiske prstiju. Da bi *anti-spyware* softver bio što efikasniji, morate stalno ažurirati bazu podataka s potpisima. Morate također redovito skenirati svoje računalo da biste bili sigurni kako *spyware* nije pronašao put do njega. Ako možete, skenirajte bar jednom tjedno.

Možda ćete htjeti skenirati svoje računalo prije provođenja osjetljivih *online* transakcija, kao što su Web-temeljene bankarske ili druge financijske transakcije. Kao što smo govorili u 2. poglavlju, lopovi identiteta pokušavaju posijati *spyware* ili trojanske konje na vaše računalo da bi ukrali informacije za prijavu i lozinke, pa čak i da bi sami provodili transakcije. Moći ćete se ugodnije osjećati prilikom svojih *online* transakcija ako prije toga provedete skeniranje. Neke su tvrtke počele nuditi besplatno skeniranje za *malware* svojim klijentima prije nego što počnu vrijedne financijske transakcije.

Što *anti-spyware* ne može?

Budući da se *anti-spyware* softver temelji na potpisu, njemu je potrebna kopija poznatog *spyware* da bi kreirao otisak prsta. Poput AV softvera, *anti-spyware* softver ne jamči zaštitu od inficiranja vašeg računala novim *spywareom.*

Anti-spyware softver ne nudi potpunu zaštitu od svih klasa *malwarea.* Anti-spyware i AV proizvodi počeli su se poklapati, a samo *anti-spyware* softver nije dovoljan za zaštitu od virusa, crva i trojanskih konja. Uz to, *anti-spyware* proizvodi ne mogu skenirati e-poštu, koja postaje popularan put širenja zaraze za *spyware.* Za potpunu zaštitu koristite AV i *anti-spyware* softver.

Budite oprezni s besplatnim softverom

Internet vrvi besplatnim softverom, uključujući igre, programe za razmjenu datoteka, čuvare ekrana itd. Neki od njih prilično su bezopasni, ali neki nisu. Tvrtke često nude "besplatan" softver koji uključuje *adware* ili *spyware.* Trebali biste biti oprezni s ponudama besplatnog softvera. Ako softver ne obuhvaća EULA-u, izjavu o privatnosti i jasne upute kako ga kasnije možete ukloniti, tada je bolje da ga ne preuzimate.

Pročitajte EULA-u

End User License Agreement – EULA (Ugovor o licenci za krajnjeg korisnika) je ugovor između vas i proizvođača softvera. Kada preuzmete i instalirate softver, pojavit će se ekran koji uključuje EULA-u. Softver vam ne dopušta da nastavite instaliranje dok ne kliknete gumb čime potvrđujete da ste pročitali i da prihvaćate uvjete u ugovoru. Većina korisnika jednostavno klikne gumb bez čitanja licence.

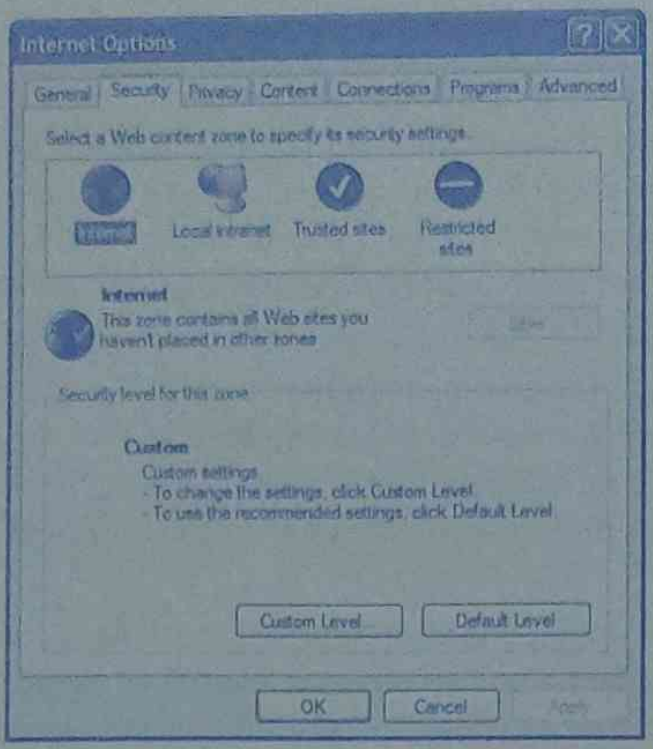
To je pogrešno, naročito ako se radi o besplatnom softveru, jer on često uključuje *adware* ili druge nepoželjne programe. Legitimne tvrtke koje nude besplatan softver informiraju vas o prisutnosti *adwarea* negdje u EULA-i (vjerojatno pri kraju) i pružaju vam opciju da odbijete cijeli paket. Ako razumijete da prihvaćanje besplatnog softvera znači i prihvaćanje *adwarea*, možete nastaviti preuzimanje softvera.

Ako pročitate EULA-u i ne naiđete na spominjanje programa ili funkcija koje nadziru vaše korištenje računala, pa poslije otkrijete da softver uključuje nepoželjne programe, taj biste softver trebali prijaviti FTC-u. FTC is ima ovlasti da poduzme mjere protiv tvrtki koje se bave prijevarnim radnjama. Detalje o ispunjavanju prijava naći ćete u odjeljku "Korisni izvori" na kraju ovog poglavlja.

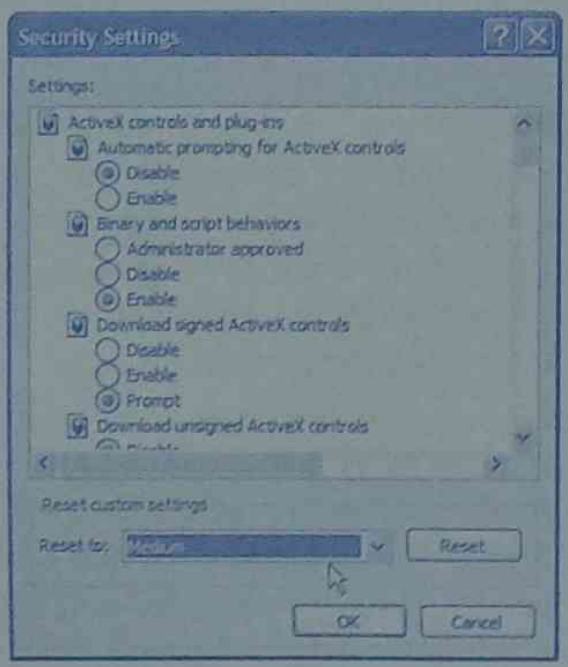
Podesite postavke svojeg pretraživača

Možete podesiti postavke IE pretraživača tako da vas on upozori kada se neka ActiveX kontrola želi učitati na vaše računalo i omogućuje vam da prihvatite ili odbijete njezino preuzimanje. Da biste provjerili ovu postavku, otvorite IE i odaberite Tools, Internet Options, a zatim kliknite jahač Security. Vidjet ćete četiri Web zone za koje možete podesiti postavke sigurnosti: Internet, Local intranet, Trusted sites i Restricted sites, kao što je prikazano na slici 5.4.

Da biste promijenili postavku svake zone, kliknite ikonu zone koju želite podesiti pa kliknite gumb Custom Level. Otvorit će se novi prozor pod nazivom Security Settings (slika 5.5). Možete odrediti pojedinačna pravila za rad s ActiveX kontrolama ili jednostavno odabrati postavku Medium pri dnu dijaloškog okvira. Tako dugo dok je postavka IE Security postavljena na Medium, dobit ćete poruku upozorenja; svaka druga postavka dopušta ActiveX kontrolama da se učitaju na vaše računalo bez vašeg znanja. (Kao što je prije spomenuto, sigurnost pretraživača detaljno je opisana u 7. poglavlju.)



Slika 5.4 Opcije Internet Security



Slika 5.5 Dijaloški okvir Security Settings

Na žalost, čak i ako vas dijaloški okvir upozori na preuzimanje, klik gumba No neće uvijek pomoći. Neki pisci *malwarea* manipuliraju tim dijaloškim okvirom tako da će se softver i ako kliknete No ili neki drugi gumb svejedno učitati. Napadači pokušavaju oponašati poruke da izgledaju kao one s vašeg sustava Windows,

za razliku od ActiveX kontrola, ili da izgledaju kao da ih generira Web lokacija na kojoj se nalazite. Te su poruke obično alarmantne i traže da odmah nešto poduzmete, kao što je klik gumba Yes za provođenje skeniranja ili preuzimanje programa koji će riješiti "problem". Takve biste poruke trebali ignorirati.

Da biste zatvorili dijaloške okvire i iskočne okvire bez klika gumba No, Cancel ili X možete pritisnuti kombinaciju tipki Alt-F4. Tako ćete sigurno zatvoriti prozore unutar pretraživača bez preuzimanja ikakvih programa.

Koristite neki alternativni pretraživač

Druga opcija pomoći za zaštitu od kopiranja *spywarea* na vaše računalo je korištenje pretraživača koji nije Internet Explorer. Na primjer, Firefox i Opera ne koriste ActiveX, što sprječava ActiveX-temeljene zlonamjerne programe da utječu na vaše računalo. Ti pretraživači su također rjeđe podvrgnuti provalama kroz njihove pukotine (djelomično zato jer nisu ni približno toliko široko rasprostranjeni kao Internet Explorer, a pisci *malwarea* idu na inficiranje najčešće korištenih aplikacija kako bi zarazili što je moguće više računala). Ali, alternativni pretraživači nisu neranjivi. (Na primjer od srpnja do prosinca 2004. godine postojala je 21 sigurnosna mna Mozilla pretraživača u usporedbi s 13 mana Microsoft Internet Explorera.) Zato, ako koristite jedan od ovih pretraživača, trebali biste redovito preuzimati ažurirane verzije. Mogli biste i otkriti da neke Web lokacije ne rade tako dobro s alternativnim pretraživačima.

Da biste preuzeli pretraživač Firefox Web otiđite na lokaciju www.mozilla.org. Za preuzimanje pretraživača Opera otiđite na lokaciju www.opera.com.

Stalno ažurirajte svoj softver

Ažuriranje softvera je računalni ekvivalent konzumiranja povrća: ono je osnova da dobro zdravlje, pa ga morate redovito jesti. Novi *spyware* i *adware* programi stalno se kreiraju, kao i novi potpisi na njihovo otkrivanje. Zato je važno da ažurirate svoj sigurnosni softver. Većina programa dopušta da vam se ažurirane verzije automatski isporučuju putem Interneta.

Isto vrijedi i za vaš operativni sustav i aplikacijske programe. Kao što smo prije spomenuli, Microsoft izdaje ažurirane verzije, koje se nazivaju i zakrpe, svakog drugog utorka u mjesecu. U 7. poglavlju objašnjavamo kako postaviti računalo da automatski preuzima Microsoftove zakrpe. Drugi proizvođači također izdaju nove ažurirane verzije softvera da bi riješili pukotine koje bi mogle omogućiti napadačima da naštete ili upravljaju vašim računalom.

5.5 Kako ukloniti *spyware*, *adware* i trojanske konje?

Ako pratite sve korake prevencije koji su ovdje opisani, moći ćete držati većinu *spywarea* i trojanskih konja podalje od svojeg stroja. Ali i dalje postoji mogućnost da se neki programi uvuku pokraj obrane, pa je važno da znate koji su znakovi zaraze i kako ukloniti nepoželjne programe.

Najbolje je riješiti se nepoželjnog softvera upotrebom *anti-spyware* antivirusnih alata. Ti alati pretražuju vaše računalo u potrazi za bilo kakvim tragovima poznatog *spywarea*, *adwarea* i trojanskih konja. Kada jednom pronađu te tragove, moći ćete odabrati hoćete li izbrisati, onemogućiti ili ostaviti odnosne programe. *Spyware* i trojanske konje možete i ručno ukloniti, pomoću alata dostupnih na Internetu.

Kako prepoznati zaraženo računalo?

Kao i kod virusa i crva, najbolji način da provjerite je li vam računalo zaraženo *spywareom*, *adwareom* ili trojanskim konjima je da upotrijebite *anti-spyware* i antivirusni softver. Ti programi otkrivaju prisutnost nepoželjnog softvera na vašem stroju i pružaju opcije da nešto s njima učinite. Trebali biste redovito skenirati svoje računalo za obje vrste softvera te isto tako osigurati da sigurnosni softver redovito skenira računalo za obje vrste softvera te da se izvodi dok surfate Internetom.

Ako još nemate vlastiti *anti-spyware* softver, možete dobiti uslugu besplatnog skeniranja od raznih *anti-spyware* proizvođača. Webroot Software nudi besplatno skeniranje pod nazivom Spy Audit, koje možete pronaći na polaznoj stranici tvrtke na adresi www.webroot.com. Zone Labs na lokaciji www.zonelabs.com i Symantec na www.symantec.com, također pružaju skeniranje *spywarea*. Computer Associates nudi besplatno skeniranje na adresi www.ca.com. Kliknite vezu Products ispod popisa Home and Home Office pa kliknite eTrust PestPatrol. To će vas odvesti na stranicu za pokretanje skeniranja. Besplatno skeniranje možete dobiti i od tvrtke Aluria Software odlaskom na adresu www.aluriasoftware.com. Mnoga ta skeniranja koriste ActiveX kontrole pa ćete morati klikanjem proći kroz ekrane upozorenja u svojem Internet Exploreru.

Možete i potražiti sljedeće znakove:

- Je li vaše računalo zatrpano oglasima?
- Mijenja li se vaša polazna Web stranica svaki put, čak i kada je vratite na prvobitni prikaz?

- Jeste li preusmjereni na nepoznate tražilice na koje niste kliknuli?
- Je li vaše računalo svojevoljno, naročito kada surfate Webom? *Spyware* i *adware* koji prate vaše aktivnosti koriste vašu vezu s Internetom za slanje izvještaja i usmjeravanje oglašavanja na vaše računalo. Takvo ponašanje smanuje propusnost vašeg pristupa Internetu i utječe na brzinu pri kojoj se Web sadržaj isporučuje. *Spyware* i *adware* također koriste CPU (centralnu procesorsku jedinicu) vašeg računala. Ako na vaš stroj dospije dovoljna količina *spywarea* i *adwarea*, taj se softver natječe za preuzimanje snage obrade s drugim aplikacijama i utječe na cjelokupnu brzinu pri kojoj vaše računalo provodi normalne funkcije. U mnogim slučajevima, zaraženo računalo jednostavno prestaje biti operativno.
- Ruši li vam se računalo često?
- Iskaču li na vašem računalu oglasi čak i kada niste ne Internetu?
- Vidite li novu alatnu traku u svojem Web pretraživaču?
- Jeste li vi ili netko tko koristi vaše računalo preuzeli "besplatne" programe poput onih za dijeljenje datoteka, praćenje vremenske prognoze, čuvare ekrana ili pomoćne programe koji jamče poboljšano *online* iskustvo?
- Je li vaš vatrozid otkrio programe na računalu koji pokušavaju pristupiti Internetu?

Korištenje alata HijackThis

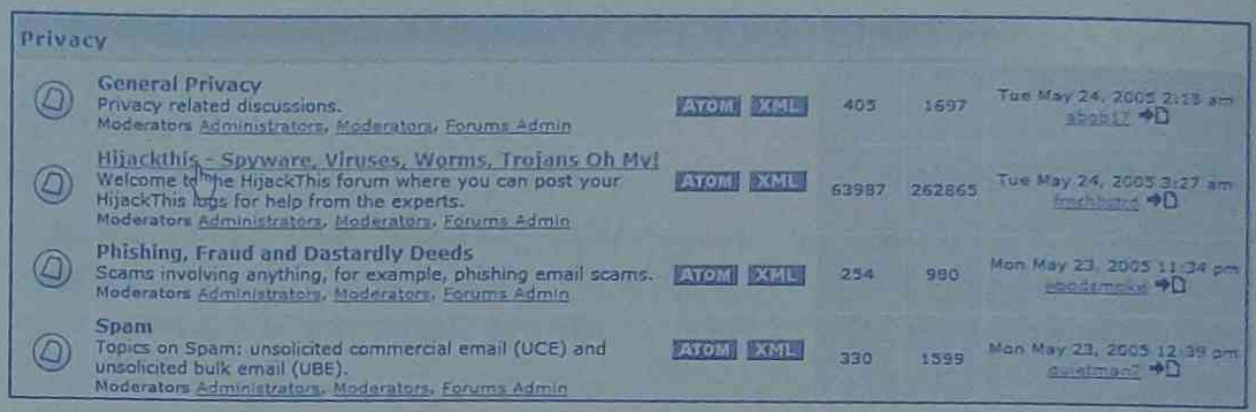
Da biste ručno ukloniti nepoželjne programe sa svojeg računala, morate izbrisati datoteke i unose tih programa u Registryu. To od vas zahtijeva da znate koje je promjene *spyware* proveo u postojećim ključevima Registrya i koje je nove ključeve u njega instalirao.

Popularan alat za uklanjanje otimača pretraživača iz Registrya je HijackThis. On skenira vaš Registry i daje vam popis (koji se naziva dnevnik ili log) sadržaja. Tada možete odabrati koji sadržaj ukloniti. Kopiju alata HijackThis možete pronaći na lokaciji njegovog tvorca: www.merijn.org/downloads.html. (One je i tvorac CWShreddera, popularnog alata za uklanjanje CoolWebSearcha. CoolWebSearch je jedan od najupornijih i brzo razvijajućih komada *spywarea* na Internetu. CWShredder je besplatno dostupan na adresi www.merijn.org/downloads.html.)

HijackThis je ručni alat, što znači da ćete sami morati ukloniti nepoželjni sadržaj. Za razliku od većine komercijalnih *anti-spyware* programa, HijackThis

ne nudi savjet o tome što biste trebali ukloniti. Toplo se preporuča da potražite pomoć prilikom odlučivanja koje dijelove Registrya trebate ukloniti. Ako prilikom mijenjanja svojeg Registry pogriješite, vaše računalo možda neće ispravno raditi. Ako imate ugovor o podršci s nekom AV ili *anti-spyware* tvrtkom ili sa proizvođačem svojeg računala, oni bi vam mogli pomoći oko HijackThis dnevnika.

Alternativno, besplatnu pomoć za HijackThis dnevnik možete dobiti na brojnim *online* forumima. Te forume vode napredni korisnici koji vam mogu pomoći u pregledavanju dnevnika i provođenju promjena. Jedan popularan forum je CastleCops. Otiđite na lokaciju www.castlecops.com i kliknite gumb Forums pri vrhu stranice, pa se pomaknite prema dolje do odjeljka Privacy i kliknite unos HijackThis – Spyware, Viruses, Worms, Trojans Oh My! kao što je prikazano na slici 5.6. Svakako pročitajte smjernice za korištenje foruma i slanje HijackThis dnevnika. CastleCops ima i tehnički praktični vodič za HijackThis na adresi http://castlecops.com/HijackThis.html.



Slika 5.6 CastleCopsov HijackThis forum.

Druga opcija je SpywareInfo na adresi www.spywareinfo.com. Na polaznoj stranici možete se pomaknuti prema dolje do sekcije pod nazivom The Browser Hijacker Articles. Veze u ovoj sekciji nude informacije o tome kako se koristi alat HijackThis. Možete se i registrirati za slanje svojeg dnevnika ili pitanja na korisnički forum. Ona također sadrži veze do drugih *online* foruma na kojima možete pregledati svoj HijackThis dnevnik.

Dnevnik možete poslati i na Spyware Warrior logs na adresi www.merijn.org.

Preformatiranje tvrdog diska

U najgorem slučaju, *anti-spyware* softver neće moći ukloniti nepoželjne programe pa ćete trebati zatražiti nečiju pomoć. Ako ste kupili *anti-spyware* softver, kontaktirajte službu za podršku korisnicima da čujete što oni preporučuju (ali budite spremni na dugo čekanje). Mogli biste i kontaktirati proizvođača svojeg računala, potražiti pomoć u trgovini u kojoj ste ga kupili (uz naknadu, naravno) ili kontaktirati lokani servis za računala.

Kao posljednju opciju imate da započnete od nule i jednostavno ponovno instalirate operativni sustav i aplikacije koristeći originalne diskove sa softverom. Za to jednostavno umetnite originalni disk svojeg operativnog sustava u CD-ROM pogon i pokrenite računalo. Ono traži da ponovno potvrdite želju za reinstaliranjem operativnog sustava. Međutim, reinstaliranje operativnog sustava briše sve podatke koje ste spremili na računalo (nadajmo se da imate dobre navike kreiranja sigurnosnih kopija). To je posljednja opcija; prije nego što počnete formatiranje tvrdog diska iscrpite sve druge opcije.

5.6 Popis za provjeru

Upotrijebite ovaj popis kao brzi referentni vodič za materijal iznesen u ovom poglavlju.

Učinite

- Koristite *anti-spyware* softver i održavajte ga ažurnim.
- Podesite postavke svojeg pretraživača da vas obavještava o ActiveX preuzimanjima.
- Pročitajte EULA prije nego što preuzmete bilo koji softver na svoje računalo.
- Budite pažljivi s besplatnim softverom.
- Održavajte svoje namjenske programe (aplikacije) i operativni sustav ažurnima.
- Provodite redovito kreiranje sigurnosnih kopija bitnih datoteka.

Nemojte učiniti

- Nemojte dopustiti učitavanje nepoželjnog softvera.
- Nemojte klikati iskočne oglase ili nepozvane i alarmantne iskočne poruke koje tvrde da imate *spyware* ili druge probleme s računalom.

- Nemojte prihvaćati priloge e-pošte od stranaca.
- Nemojte otvarati poruke e-pošte koje tvrde da dolaze iz neke financijske institucije ili lokacije za e-trgovinu s kojima ne poslujete.
- Nemojte prihvatiti softver bez čitanja EULA-e.
- Nemojte se bojati isprobati novi Web pretraživač.

5.7 Korisni izvori

Ovaj odjeljak predstavlja dodatne izvore koji će vam pomoći da više naučite.

Ben Edelman je student prava na Harvard Universityju i jedan od istraživača *anti-spywarea*. Njegova je Web lokacija puna odličnih informacija o praksama varanja isporučitelja *adwarea*, o načinima na koje programi koriste pukotine u sigurnosnim sustavima i kritikama donošenja *anti-spyware* zakona. Njegove članke možete pročitati na lokaciji www.benedelman.org.

Spyware Warrior je informativna lokacija o svim stvarima vezanim uz *spyware*, koju vodi Eric Howes. Ako tražite neki *spyware* proizvod, provjerite vezu koja uspoređuje razne *anti-spyware* softvere uključujući i one besplatne. Veza do Spyware bloga vodi vas na Web log s pregrštom trenutnih informacija o novom *spywareu* i razvojima u *anti-spyware* zajednici. Možete se i pridružiti brojnim forumima i slati HijackThis dnevnike.

PC Pitstop nudi dijagnostičke alate za PC-e i pruža korisne informacije o *spywareu*. Na primjer, provjerite njegove ocjene prvih 25 *spyware* i *adware* programa na adresi http://www.pcpitstop.com/spycheck/top25.asp.

Merijn Bellekom je autor alata HijackThis, CWShredder i drugih korisnih *anti-spyware* alata, a sve ih možete preuzeti s Web lokacije www.merijn.org.

Spywareinfo.com je nabijen dobrim informacijama. Ako želite doznati više o *spywareu*, kolačićima, otmicama pretraživača i drugome, kliknite gumb More Links na polaznoj stranici. Lokacija također preporučuje proizvode koji će vam pomoći u rješavanju problema s nepoželjnim softverom. Ako se registrirate na lokaciju, moći ćete slati pitanja na oglasnu ploču i dobiti pomoć oko rješavanja problema sa *spywareom* (ali najprije svakako pročitajte FAQ). Možete se i pretplatiti ne bilten koji piše Mike Healan, tvorac lokacije.

Da biste pročitali kopiju FTC-ovog izvještaja iz ožujka 2005. godine o *spywareu*, otiđite na adresu www.ftc.gov/os/2005/03/050307spywarerpt.pdf. Da biste FTC-u podnijeli tužbu protiv *spywarea* ili *adwarea* otiđite na adresu www.ftc.gov i kliknite vezu File a Complaint na polaznoj stranici. Spywareguide.com ima bazu

podataka poznatog *spyware* i *adware* koja se može pretraživati. Na polaznoj stranici, u traku za pretraživanje možete upisati ime programa da provjerite nalazi li se on na popisu. Lokacija također ocjenjuje *spyware* programe prema razinama opasnosti od 1 do 10, uz opis svake razine.

Čitanje teksta napisanog malim slovima

Kazaa, koja proizvodi softver za izravnu razmjenu datoteka putem Interneta uključuje i *adware* u besplatnoj verziji svojeg proizvoda. Naravno, softver je besplatan jer se vi slažete da preuzimate i *adware* koji generira ciljano oglašavanje.

Tvrtka to objašnjava u EULA-i, koji možete pročitati na adresi www.kazaa.com/us/terms2.htm. Odjeljci o *adware* napisani su pri dnu EULA-e u odjeljku Section 9. Od sredine 2005. godine Kazaa je upakirala pet *adware* programa uključujući Cydoor, program za isporuku oglasa koji, prema EULA-i tvrtke, "koristi vašu Internet vezu za ažuriranje svojeg izbora dostupnih oglasa i pohranjuje ih na vaš tvrdi disk".

Uključen je i GAIN AdServer, koji prema EULA-i tvrtke, "identificira vaše interese na temelju vašeg korištenja računala i koristi te informacije da vam isporučuje oglašivačke poruke".

Kazaain EULA uključuje i veze do EULA-ova za Cydoor i GAIN AdServer i kaže da preuzimanjem Kazaae vi prihvaćate EULA-ove za svaku od ovih softverskih komponenti.

Uz to EULA zahtijeva da ne koristite nikakav drugi softver koji će onemogućiti ili blokirati oglase koje isporučuju ove komponente, jer će u protivnom Kazaa prekinuti funkcioniranje.

Što biste zapravo trebali učiniti ako zaista želite koristiti besplatan softver za dijeljenje datoteka? Može razmisliti o tome što dobivate i što gubite. Tako dugo dok ste spremni snositi posljedice koje dolaze s *adwareom* (dosadne oglase i potencijalno lošije performanse računala) softver možete preuzeti i početi dijeliti datoteke.

6. poglavlje

Recite 'ne' *spamu*

Spam ima jednu namjenu: generirati prihod za one sumnjivog morala. Kao i s visokorizičnim *adwareom* i *spywareom*, borba protiv *spama* je teška jer *spameri* imaju financijske poticaje da budu uporni i inovativni. Rezultat je stalna igra dobivanja prednosti između frakcija "za" i "protiv" *spama.* U jednu ruku *spameri* pokušavaju sve: manipuliranje sustavima za e-poštu, tehnološki sofisticirane napade koji poražavaju *spam* filtre i brutalnu silu poplavljivanja *junk* porukama e-pošte koja nastoji poraziti obranu samom količinom. U drugu pak ruku, razvijene su i profinjene nove tehnologije za izbjegavanje *junk* poruka e-pošte, izglasani su zakoni za progonjenje i tuženje *spamera*, a korisnici postaju mudriji prilikom izbjegavanja *spama.*

U danima kada je Internet počeo privlačiti široku korisničku publiku, *spam* je žestoko osakatio e-poštu i gotovo je ubio. Danas, za većinu kućnih korisnika, *spam* je više gnjavaža nego prijetnja. Zahvaljujući naporima onih koji razvijaju softver, pružatelja usluga i odlučnih *anti-spam* zajednica, većina se *spama* filtrira na ulazu i nikada ne dolazi u vaš poštanski sandučić. Davatelji Internet usluga (ISP-ovi) kao što su AOL i Comcast, i pružatelji Web pošte kao što su Yahoo!, MSN i Google, osiguravaju da njihovi korisnici dobivaju prilično čist dotok poruka. Upitne poruke prosljeđuju se u mape za masovne poruke (*bulk mail*) da biste ih mogli pregledati, a očigledni *spam* se ubija bez isporuke.

Uz sve ovo, *spam* ne pokazuje znakove odustajanja. Za svaki napredak u *anti-spam* tehnologiji dolazi i kontra napredak u tehnikama masovnog slanja poruka. Približno 30 milijardi poruka e-pošte dnevno šalje se Internetom, a konzervativne procjene govore da barem 50% tih poruka čini *spam.* (Druge procjene iskazuju da *spam* čini 90% cjelokupne e-pošte.) Možete misliti da se to vas malo tiče, jer *junk* poruke nikada ne dospijevaju u vaš poštanski sandučić. Zapravo, 15 milijardi (ili više) *junk* poruka stvara značajne troškove za javne operatore i davatelje usluga. Svaka *junk* poruka koja putuje Internetom guta resurse kao što je propusnost na linijama od optičkih vlakana i sposobnosti obrade usmjernika i poslužitelja e-pošte koji poruke prosljeđuju s jednog na drugo mjesto. Javni operatori i davatelji usluga moraju također investirati u softver za obradu i analizu dolaznih poruka, te moraju naručiti još veće količine hardvera koji će raditi s takvim obimom pošte. Ti se troškovi prenose vama u obliku viših mjesečnih naknada.

Tehnike masovnog slanja poruka usvojili su i pisci virusa i *malwarea,* koji su uvijek u potrazi za novim načinima širenja svojih podmuklih kreacija. Nova verzija *spama* koja se naziva *phishing* šalje *bulk* e-poštu da bi se navelo ljude na otkrivanje informacija o bankovnim računima. Zato *spam* više nije samo gnjavaža, on može biti itekako opasan.

A problem neće nestati tako dugo dok postoje dva uvjeta. Prvi, *spamerima* se još uvijek lako skrivati. Zahvaljujući tehnikama zakrivanja e-pošte, *spameri* mogu prikriti izvor svoje *junk* pošte. Internet je također prepun nezaštićenih strojeva, bilo poslužitelja e-pošte ili kućnih računala, koje *spameri* mogu oteti i koristiti ih kao nehotične *spam* generatore. Svijet je isto tako pun davatelja usluga koji su voljni okrenuti glavu kada su u pitanju klijenti koji generiraju tisuće ili stotine tisuća poruka dnevno – tako dugo dok ti klijenti uredno podmiruju svoje račune.

Drugo, *spam* će postojati tako dugo dok lakovjerni ljudi odgovaraju i zapravo kupuju oglašene proizvode i usluge ili postaju žrtve razmnožavanja *scamova.* Ovo poglavlje daje kratak pregled *spam* ekonomije, načina rada *spamera* i alata koje koriste *anti-spameri,* internog djelovanja infrastrukture e-pošte i korisnih savjeta da ne biste postali žrtvama *junk* pošte. Pregledat ćemo i nekoliko proizvoda koji vam mogu pomoći da držite *spam* podalje od svog računala.

6.1 *Spamonomija*

Spam je igra za novac i zato poštuje jednostavne ekonomske principe: tako dugo dok je prihod dobiven od *spama* veći od troška njegova slanja, *spam* će postojati. Kao oblik oglašavanja, *spam* je najjeftiniji postojeći oblik. Želite li prodavati magične tablete za mršavljenje preko nekog drugog medija, morat ćete unaprijed plaćati značajne novčane iznose za oglašavanje. Ali slanje 100.000 poruka e-pošte na dan stajat će vas koliko i veza s Internetom, nekoliko računala i neki generički *spam* softver (da, možete kupiti *spam* softver – na Internetu, naravno).

Spameri dobro zarađuju. Uzmimo primjer pošiljatelja *junk* e-pošte Jeremyja Jaynesa. On je u studenom 2004. godine optužen na 9 godina zatvora za slanje velike količine nepoželjnih poruka e-pošte i falsificiranje informacija o usmjeravanju u porukama kako bi od primatelja tih poruka prikrio svoje identitet. Jaynes je vodio nekoliko prljavih *spam* poslova uključujući prodaju pornografskih materijala, softvera za privatnost, usluge za "ubiranje novca" te shemu rada od kuće. Prema sudskim dokumentima Jaynesove operacije slanja gomila poruka e-pošte generirale su mjesečno 10.000 kupovina kreditnim karticama. Premda je dvije trećine onih koji su kupili neki proizvod tražilo povrat novca, Jaynes je imao neto profit od preko 100,000 američkih dolara mjesečno. Tužitelji su procijenili da je njegov ukupni neto prihod iznosio približno 24 milijuna dolara.

Naravno, da bi *spamonomija* funkcionirala moraju postojati kupci i prodavači. Jedini razlog zbog kojeg *spam* opstaje je taj da netko negdje zapravo kupuje nešto *junk* poštom. Taj bi element mogao biti jedan od nerješivih aspekta problema sa *spamom*. Softver za filtriranje *spama* može se stalno poboljšavati, ali čini se da je ljudska naivnost (ili obična glupost) konstantan problem. Ljudi koji zapravo odgovaraju na *spam* poruke mogu biti obrazovaniji nego što mislite. 2004. godine, studija tvrtke Pew Internet & American Life Project otkrila je da je 5% korisnika Interneta kupilo neki proizvod oglašen u nepoželjnoj poruci e-pošte. Iste je godine udruga Business Software Alliance objavila rezultate istraživanja u kojima stoji da je 21 posto ispitanika iz SAD-a naručilo nešto iz *spam* oglasa.

Pa da vidimo što ljude potiče da odgovaraju na *spam* ponude? Nisam psiholog, ali imam nekoliko teorija:

- *Spam* cilja na osnovne ljudske želje. *Spam* obično cilja na: seks (pornografija, Viagra), novac (piramidne sheme, jeftine hipotekarne kredite, sheme s novcem od nigerijske nafte) i želju za poboljšanjem vlastitog imagea (gubitak tjelesne težine, povećanje penisa i jeftinu robu prestižnih dizajnera).

Zapravo, gumbi koje *spameri* pokušavaju pritisnuti isti su kao i oni vodećih marketinških agencija. Internet *spameri* i tvrtke iz Madison Avenuea ostvaruju profit od naše preokupacije vlastitim financijama, vlastitim imageom i dokazivanjem seksualnosti. Ono što *spamere* čini drugačijima je to što oni jeftino oglašavaju, teško ih je otkriti i njihove su metode često ilegalne, a uz to će vas naravno pokušati orobiti.

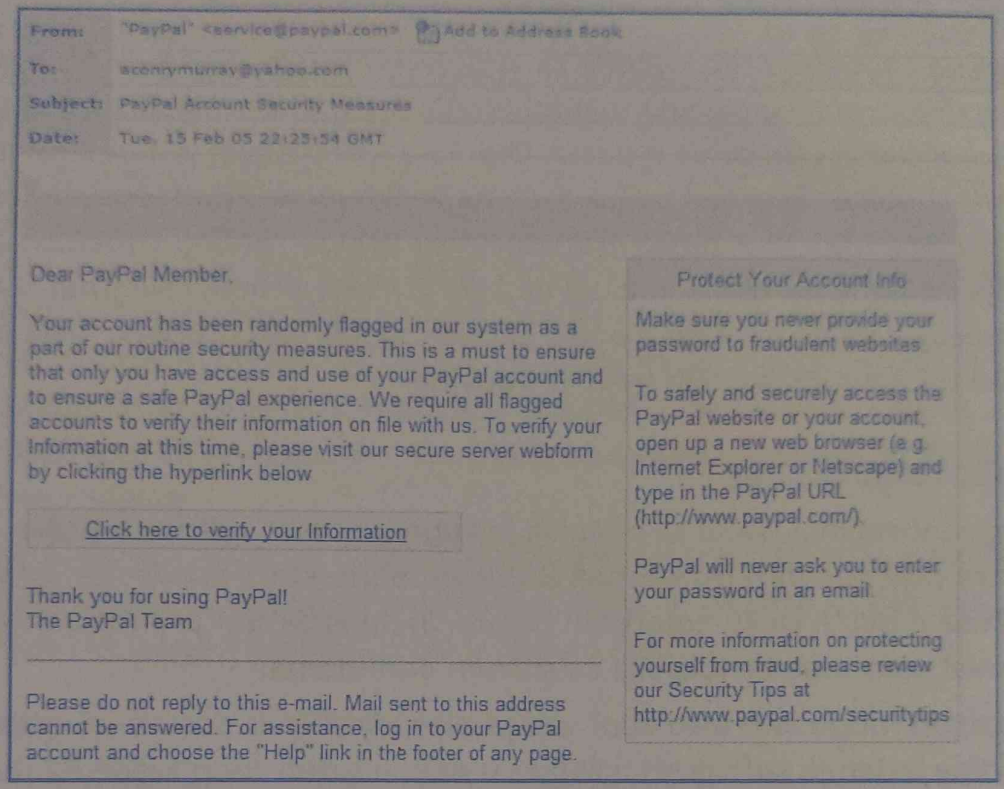
- *Spam* pruža dozu anonimnosti. Osoba koja se srami u trgovini kupiti pornografske materijale ili paket za povećanje penisa prihvatit će pseudo-anonimnost Internet ponude. Netko tko ne želi od svojeg doktora tražiti recept za Viagru može se sam "liječiti" zahvaljujući *spamu.* Osoba koja ne bi kupila piratski softver iz nečijeg prtljažnika mogla bi to učiniti putem Interneta. Usamljeni ekran računala i naizgled eteričan medij internetskih komunikacija može ublažiti strah od javne sramote koji oblaže (ili je supstitut za) našu bolju prirodu.

6.2 *Spam, scamovi* i *phishing*

Dok tradicionalan *spam* i dalje postoji (pod tradicionalnim smatram nepoželjne poruke e-pošte koje pokušavaju nešto prodati), kriminalci se često oslanjaju na varijante *spama* da bi uhvatili lakovjerne primatelje u razne zamke. Najpoznatiji *scam* je onaj s nigerijskom naftom, u kojem pošiljatelj tvrdi da ima milijune dolara koje pokušava prenijeti iz Afrike. (Ta se kategorija naziva i 419 *scamovi* po nigerijskoj šifri za presudu.) Pošiljatelj obećaje da će velikodušno prenijeti dio novca na vaš bankovni račun, ali prije toga vi trebate poslati novac za razne "naknade" i ostale stvari. Drugi popularni *scam* e-pošte je međunarodna lutrija – možete podići svoju nagradu nakon što uplatite malu administrativnu naknadu (i kad na vrbi rodi grožđe). Bit ove vrste *scama* (ili gomile varijanti) je ta da mislite kako ćete za ništa dobiti nešto. Istina je potpuno suprotna.

Druga i potencijalno mnogo opasnija varijanta *spama* naziva se *phishing* (pecanje). U 2. poglavlju "Sprječavanje krađe identiteta", objasnili smo *phishing,* ali ćemo ga ovdje ponovno objasniti u slučaju da ste preskočili to poglavlje.

Phishing napadi počinju porukom e-pošte (koja se šalje na mnoštvo adresa) u kojoj piše da je od banke, kompanije za izdavanje kreditnih kartica, ISP-a ili tvrtke za e-trgovinu (eBay i PayPal su dvije popularne mete). Neka je *phishing* e-pošta očigledna prijevara, ali neke poruke su zaista remek-djela, s logotipom kompanije i pisane jezikom korporativnog marketinga.



From: "PayPal" <service@paypal.com> Add to Address Book
To: aconrymurray@yahoo.com
Subject: PayPal Account Security Measures
Date: Tue, 15 Feb 05 22:25:54 GMT

Dear PayPal Member,

Your account has been randomly flagged in our system as a part of our routine security measures. This is a must to ensure that only you have access and use of your PayPal account and to ensure a safe PayPal experience. We require all flagged accounts to verify their information on file with us. To verify your information at this time, please visit our secure server webform by clicking the hyperlink below

Click here to verify your Information

Thank you for using PayPal!
The PayPal Team

Please do not reply to this e-mail. Mail sent to this address cannot be answered. For assistance, log in to your PayPal account and choose the "Help" link in the footer of any page.

Protect Your Account Info

Make sure you never provide your password to fraudulent websites.

To safely and securely access the PayPal website or your account, open up a new web browser (e.g. Internet Explorer or Netscape) and type in the PayPal URL (http://www.paypal.com/).

PayPal will never ask you to enter your password in an email.

For more information on protecting yourself from fraud, please review our Security Tips at http://www.paypal.com/securitytips

Slika 6.1 Lažna e-pošta PayPala

Phishing e-pošta uglavnom sadrži alarmantnu poruku u kojoj piše da postoji problem s vašim računom koji se odmah mora riješiti. Ta poruka uključuje nešto što izgleda kao veza na stranicu za prijavu na Web lokaciju. Ako kliknete vezu, naći ćete stranicu za prijavu koja izgleda identično onoj prave lokacije s poljima za unos korisničkog imena i lozinke te broja računa. Mnoge *spoofirane* lokacije postaju toliko pohlepne da traže i druge informacije poput matičnog broja. Vi, žrtva, u želji da riješite sve probleme sa svojim računom marljivo ćete upisati te informacije i kliknuti Send. Vaše su informacije upravo ukradene.

Kao da nisu dovoljno zli, *phisheri* postaju sve mudriji. Mnogi u svoje poruke e-pošte ili na Web lokaciju na koju vas šalju uključuju zlonamjerne programe, kao što su virusi, *keystroke loggeri* i trojanski konji (pročitajte 4. i 5. poglavlje).

U nekim je slučajevima dovoljno da jednostavno otvorite poruku e-pošte i *malware* će se učitati na vaše računalo. Zato, čak i ako ne padnete na neki *phishing scam*, vaše bi računalo moglo biti inficirano.

6.3 Kako rade *spameri*?

Spameri koriste razne metode za igranje svoje igre. Neke od tih metoda tehnički su sofisticirane i uključuju manipuliranje Internet protokolima koji se koriste za isporučivanje i praćenje e-pošte. Drugi su jednostavni poput kupnje CD-a s adresama e-pošte. *Spameri* uvijek rade na veliko jer se *spam* poruka teško probija kroz razne filtre koje postavljaju davatelji usluga i krajnji korisnici. Zato *spameri* šalju milijune poruka u nadi da će 1 do 2 posto pronaći svoj put u neki poštanski sandučić i da će tih 1 do 2 posto zapravo generirati prodaju. Ovaj odjeljak opisuje neke od najuobičajenijih trikova trgovine.

Kupovanje popisa

Najjednostavniji način za početak je kupnja popisa adresa e-pošte. Na primjer, tvrtka pod imenom Bulk Email Software Superstore prodat će vam jedan milijun adresa e-pošte za 40 američkih dolara. Jednostavnim pretraživanjem Interneta pozvat ćete desetke lokacija sa sličnim ponudama.

Spameri mogu isto tako kupovati popise ukradenih adresa e-pošte. U lipnju 2004. godine jedan je softverski inženjer u AOL-u tužen zbog krađe 92 milijuna adresa korisnika AOL-a koje je preprodao *spamerima*.

Strvinari e-pošte

Na Internetu su dostupni programi koji puzu Web stranicama u potrazi za adresama e-pošte. Ti strvinari ili gmizavci skeniraju milijune stranica tražeći izdajnički znak @ i grade bazu podataka adresa e-pošte. *Spameri* i tvrtke koje prodaju proizvode *spamerima* koriste te gmizavce kao skupljače adresa.

Napad po rječniku/žetva imenika

Napad po rječniku (*dictionary attack*), poznat i kao žetva imenika (*directory harvesting*), inteligentan je pristup koji koristi brutalnu silu za slanje spama. Spamer jednostavno kreira program koji ciklički prolazi kroz varijante uobičajenih imena (John_Smith@isp.com, J_Smith@isp.com, jsmith@isp.com, Ted_Smith@isp.com), bira određenu domenu kao cilju i pokreće program. Program šalje spoine ili

tisuće ili milijune poruka e-pošte u nadi da će naciljati dovoljno ispravnih kombinacija imena kojima će se poruke isporučiti. Napad preko rječnika predstavlja ozbiljan problem jer može preplaviti ciljni poslužitelj za e-poštu i iscrpiti računalne resurse u tolikoj mjeri da se legitimna e-pošta neće moći probiti.

Krivotvorenje

Spameri iskušavaju svakakve metode da bi sakrili izvor poruke jer su davatelji usluga brzi u blokiranju izvora *spama* i zbog toga što federalni zakon CAN-SPAM znači da *spameri* mogu završiti u zatvoru ako ih se uhvati i optuži.

Kao što je prije spomenuto, SMTP je protokol za slanje e-pošte. SMTP se oslanja na dvije vrste zaglavlja pri isporučivanju pošte: zaglavlje omotnice i zaglavlje poruke. SMTP koristi zaglavlje omotnice da kaže uključenim poslužiteljima e-pošte kamo poslati poruku. Svaki poslužitelj e-pošte kroz koji prolazi poruka dodaje i vlastita zaglavlja poruke. Čitanjem zaglavlja omotnica možete vidjeti kojim je putem e-pošta prolazila na Internetu. Međutim, *spameri* mogu kreirati i lažna zaglavlja i injektirati poruke e-pošte na poslužitelje za e-poštu nadajući se da će tako zamesti svoje tragove.

Zaglavlja poruka uključuju retke To: i From: koje vidite u svojem klijentu e-pošte. Ta zaglavlja poruka lako je krivotvoriti (*spoofing*). I samo to možete učiniti tako da jednostavno umetnete lažnu adresu e-pošte u redak From:.

Spam proxyji

Spam proxyji su poslužitelji e-pošte ili računala koja su oteta za slanje *spama*. *Spam proxy* može biti neki poslužitelj e-pošte koji je krivo konfiguriran kao otvoreni prijenosnik. U drugim slučajevima, *spameri* pokušavaju posijati programe trojanskih konja na računala. Kao što je objašnjeno u 5. poglavlju "Kako se riješiti nepoželjnih gostiju?, 2. dio: *spyware*, *adware* i trojanski konji" trojanski konji su programi koji glume nevine ili korisne dijelove softvera, ali kada se instaliraju mogu napadaču pružiti potpunu kontrolu nad nekim računalom. Na primjer, u kolovozu 2003. godine varijanta "F" virusa SoBig obuhvaćala je trojanskog konja koji je dopustio *spamerima* da kompromitirano računalo pretvore u *spam* prijenosnu stanicu. PC-i sa širikopojasnim vezama popularne su mete za *spam proxy* napade zbog svojih brzih i stalnih veza s Internetom.

Spam proxyji su *spamerima* vrlo vrijedni. Oni maskiraju pravi izvor *spam* e-pošte, i kada jednom *spam proxy* dođe na crnu listu (odnosno, ISP-ovi zaustave prihvaćanje pošte s odnosnog uređaja), *spameri* jednostavno odbace *proxy* s crne liste i regrutiraju novi.

Društveni inženjering

Kada se *spamer* jednom domogne adrese e-pošte, trebat će iskopati atraktivnu poruku koja će vas navesti da je otvorite. To je mjesto u kojem društveni inženjering ulazi u igru. Društveni inženjering je pristojniji naziv za varanje ljudi. Neke *spam* poruke ne opterećuju se s društvenim inženjeringom – one znaju da želite njihovu ponudu i da ćete kupiti Viagru. Drugi *spameri* žele da otvorite i pročitate njihovu e-poštu, pa koriste atraktivne ili namjerno nejasne naslove (kao što je Hello!). *Phishing* poruke e-pošte snažno se oslanjaju na društveni inženjering jer prijevara propada ako ne vjerujete da dolazi od neke organizacije za koju se predstavlja.

Web signali/Web bugovi

Web signali, poznati i kao Web bugovi, su sićušni komadi koda kao što je HTML ili GIF (datoteka sa slikom). Kada se aktiviraju, Web signal otvara vezu s nekim poslužiteljem da bi dohvatio datoteku sa slikom. Istodobno, Web signal može prenositi informacije na Web poslužitelj. Web signali mogu se postaviti na Web stranicu ili u poruku e-pošte za praćenje ponašanja korisnika. Mnoge legitimne Web lokacije koriste Web signale u kombinaciji s kolačićima da bi analizirale ponašanje korisnika i pomogle u personaliziranju doživljaja *surfanja. Spameri* postavljaju Web signale u *spam* poruke da bi saznali jeste li poruku otvorili. To im pomaže da otkriju "živu" adresu onih koji na poruku ne odgovaraju. Web signali mogu biti sićušni poput jednog piksela što ih čini nevidljivim za ljudsko oko.

6.4 Metode za filtriranje *spama*

Nužnost je majka izuma, a to je jasan slučaj s *anti-spam* filtrima. U godinama kada su istraživači koji se bore protiv *spama* započeli svoje bitke, metode filtriranja narasle su od jednostavnih pretraživanja po ključnim riječima do složenih statističkih analitičkih alata s temeljima uzetim iz istraživanja umjetne inteligencije. Rezultat je opsežan zbir alata koje koriste *anti-spam* proizvodi da vam pomognu u otkrivanju i uklanjanju *spama.*

Svi su ti alati automatizirani; odnosno, računalo ispituje dolazne poruke i odlučuje jesu li *spam* ili *ham* ("ham" su poželjne poruke). Međutim, svaki *anti-spam* alat za filtriranje riskira pogrešno identificiranje poruke. Označavanje poželjne poruke kao *spam* poruke naziva se lažno pozitivno *(false positive).* Označavanje

spam poruke kao "ham" poruke naziva se lažno negativno *(false negative)*. Pogrešno označavanje ima za posljedicu da vi, kao krajnji korisnik, toga morate biti svjesni. Posljedica lažne negativnosti je ta da će se *spam* isporučiti u vaš poštanski sandučić. Posljedica lažne pozitivnosti je da vam se poruka koja je u redu nikada neće isporučiti.

Metode filtriranja o kojima ovdje raspravljamo mogu se često podesiti da bi se pronašla ravnoteža između maksimiziranja detekcije *spama* i istodobnog minimiziranja lažnih pozitivnosti. Glavni isporučitelji e-pošte poput Yahoo!-a i AOL-a malo su konzervativniji; odnosno oni riskiraju malo veći postotak *spam* e-pošte da bi osigurali dostavljanje svih legitimnih poruka. Na taj način većina isporučitelja pošte omeđuje svoje najbolje pretpostavke korištenjem mape "Bulk". Poruke koje računalo ne može definitivno kategorizirati usmjeravaju se u tu mapu kako biste mogli donijeti konačnu presudu.

Tehnologije popisane u ostatku ovog odjeljka uglavnom koriste davatelji usluga, tvrtke i administratori poslužitelja e-pošte. Neke pronalaze i put do *anti-spam* proizvoda za korisnike. Ako implementirate osobni filtar e-pošte na klijent e-pošte svog računala, ovaj će vam popis pomoći da razumijete alate koji se koriste za blokiranje *spama*.

Filtri sadržaja/pretraživanja po ključnoj riječi

Pretraživanja po ključnoj riječi skeniraju retke naslova i tijela poruka u potrazi za riječima ili kombinacijama riječi koje indiciraju *spam* poruku. Pretraživanja po ključnoj riječi jedna su od najstarijih i najjednostavnijih metoda borbe protiv *spama*. To je ujedno i najmanje efikasna metoda.

Iako pretraživanja po riječima pružaju granularnu kontrolu popisa riječi, opasnost od lažnih pozitivnosti je velika. Na primjer, riječ "grudi" je zabranjena, pa pretraživanje po ključnoj riječi može blokirati e-poštu o istraživanjima raka dojke ili o drugim bezopasnim temama. Pretraživanja po ključnim riječima su metoda koju *spameri* lako prevare. Mnogi *spam* alati mogu namjerno pogrešno napisati neku riječ da bi zavarali filtar, a da riječ čovjekov mozak i dalje može razumjeti, kao što je pisanje riječi "pornografija" s nulama umjesto slova o (p0rn0grafija). Varanje filtra s ključnim riječima vrijedi i za nevjerojatno velik broj varijanti riječi Viagra. Postoji mnogo načina za manipuliranje pisanja riječi Viagra – zapravo toliko mnogo da se ne isplati raditi bazu podataka svih tih varijacija i njome opterećivati poslužitelj za e-poštu. *Spam* alati koriste i druge trikove, poput umetanja HTML komentara između slova u riječima. Dok HTML nije vidljiv osobi koja čita riječ, on zavarava filtar.

Crne liste

Crne liste blokiraju poruke e-pošte koje dolaze sa specifičnih IP adresa ili domena. Dobro održavana crna lista može biti vrlo efikasna pri blokiranju poznatih izvora *spama*. Najpoznatija crna lista je Mail Abuse Prevention System (MAPS, www.mailabuse.com). Njezin popis Realtime Blackhole List (RBL) je baza podataka IP adresa poznatih poslužitelja e-pošte koji su znani kao prijateljski, ili u najmanju ruku neutralni za *spamere*. Druge poznate crne liste održavaju SpamCop (www.spamcop.net) i SpamHause (www.spamhause.org). Te liste koriste davatelji usluga, tvrtke i svatko tko ima poslužitelj e-pošte. Vaš ISP može koristiti ove ili druge crne liste kao dio svoje usluge filtriranja *spama*.

Međutim, crne liste mogu biti neučinkoviti alati. *Spameri* stalno mijenjaju IP adrese i domene, pa crna lista može vrlo brzo postati nevažeća. Uz to, kompromitirana računala ili poslužitelji e-pošte koji dođu na crnu listu mogu imati velikih poteškoća da se s nje izbrišu, jednom kad riješe problem. U međuvremenu, svaka organizacija koja koristi tu bazu podataka nastavit će blokirati e-poštu, čak i ako se ne radi o *spamu*. Pronađete li na korisnike orijentiranu crnu listu, svakako provjerite koji su kriteriji za dodavanje domena i IP adresa na listu, kako se brzo domene mogu s nje uklanjati i kako se često lista ažurira.

Bijele liste

Bijele liste su popisi provjerenih adresa e-pošte ili domena. Bijele liste su vrlo točne i nadopunjuju crne liste pružanjem granularne kontrole. Dok crna lista može blokirati glavnu domenu, bijela lista može otvarati dijelove te domene za koje se zna da šalju poželjnu poštu. Bijele su liste korisne i zato jer osiguravaju isporuku pošte s provjerenih izvora i omogućuju porukama da zaobiđu druge metode otkrivanja *spama*, štedeći vrijeme i procesorsku snagu. Mana bijelih lista je ta što ih je potrebno stalno održavati kako se adrese ili domene uklanjaju ili dodaju.

Heurističke analize

Heurističke analize provode razne testove nad ulaznim porukama. Ti testovi traže karakteristike koje su vjerojatni indikatori *spama*. Svakoj se karakteristici dodjeljuje neka *spam* vjerojatnost, te se poruci daje kumulativna ocjena *spam* vjerojatnosti na temelju rezultata testova. Na primjer, da bi se izbjeglo filtriranje po ključnim riječima, neki *spameri* ulažu slike ili HTML reference u tijelo poruke. Kada otvorite neku poruku e-pošte (koja je uvijek zamaskirana bezazlenim ili zavaravajućim predmetom), vaš klijent e-pošte prikazuje sliku. Kao što možete zamisliti (ili ste vidjeli), mnoge su te slike eksplicitno seksualne prirode. Filtri

heurističkih analiza mogu koristiti detekciju slika kao jedan od svojih testova. U kombinaciji s drugim testovima, kao što su poruke koje obuhvaćaju velike fontove, umetnuti tekst ili krivotvorena zaglavlja, te će poruke dobiti veću ocjenu vjerojatnosti od poruka u kojima piše "kamatne stope hipotekarnog kredita", ali u ostalim dijelovima ne uključuju alarm. Vaganjem raznih karakteristika, heurističke analize povećavaju uvjerenje da je poruka s visokom ocjenom vjerojatnosti *spama* zapravo *junk* poruka (i obratno). Popularni heuristički alat filtriranja za poslužitelje e-pošte je otvoreni-izvor SpamAssassin (http://spamassassin.apache.org/).

No, i heuristika može generirati lažne pozitivnosti. Uz to, moraju se kreirati novi testovi da obuhvate nove *spam* tehnike, a stariji se moraju isključiti jer postaju beskorisni. Vaš davatelj usluga vjerojatno koristi heurističke analize kao dio svojeg alata za filtriranje *spama*. Anti-spam softver osobnih računala može također koristiti heurističke analize.

Potpisi *spama*

Ova metoda posuđuje stranicu iz antivirusnog scenarija i popularna je *anti-spam* tehnika. Računalni program derivira kontrolni zbroj ili kriptografsku zbrku poznatih *spam* poruka, i kreira potpis ili otisak prsta te poruke. Kontrolni zbroj je matematička operacija koja tekstualnu poruku pretvara u numerički zbroj. Ako kontrolni zbroj primijenite na dvije identične kopije poruke, dobit ćete isti zbroj. Svaka promjena u tekstu poruke generira različit zbroj. Kontrolna suma otkrivena je kao odlična metoda za identificiranje *spama* jer *spameri* šalju tisuće istih poruka. Filtar koji se temelji na potpisu čuva kopiju potpisa trenutnih *spam* poruka i primjenjuje metodu kontrolnog zbroja na svaku ulaznu poruku. Ona ulazna poruka koja odgovara potpisu jamačno je *spam* i može se odbaciti.

Međutim, *spameri* su otkrili načine da prevare i ovu tehniku. Na primjer, mnogi alati za otkrivanje *spama* umeću nasumične nizove znakova na kraj retka s naslovom ili u samo tijelo svake poruke koju šalju. Mogu umetati i HTML komentare između riječi i slova. Oni su nevidljivi primatelju, ali će biti obuhvaćeni u funkciji kontrolnog zbroja. Postavljanjem nasumičnih elemenata u e-poštu osigurava se da će metoda kontrolnog zbroja proizvesti različitu vrijednost za poruke koje su inače identične.

Naravno, *anti-spam* zajednica uzvraća udarac korištenjem filtra za otkrivanje ovih nasumičnih umetaka i kreiranje kontrolnih zbrojeva samo najznačajnijih znakova u poruci. Najveće ograničenje tehnika *spam* potpisa je vrijeme: potpis ne vrijedi ako vam *spam* dođe prije nego što njegov potpis bude usvojen u bazu podataka.

Izazov/odgovor

Sistem izazov/odgovor se zasniva na činjenici da je *spam* automatiziran izoliranjem pošte novih pošiljatelja i od pošiljatelja zahtijeva da dovrši izazov. Ako je čovjek na drugom kraju, on ili ona će odgovoriti na izazov, a originalna će poruka s dopuštenjem ući u vaš poštanski sandučić. Ako poruka dolazi od *spamera*, adresa u retku From: je ionako krivotvorena, pa izazov nije prihvaćen. Čak i ako je *spamerova* adresa u retku From valjana, vjerojatno je iz programa pa zato nećete znati kako odgovoriti na izazov. U svakom slučaju, pošiljatelj ne uspijeva s izazovom, a pridružena pošta biva odbačena.

Izazov je obično neka vrsta rebusa ili testa koji samo čovjek može riješiti. Jedan od popularnih izazova je prikazivanje slova ili brojeva koji su izobličeni ili malo zatamnjeni, ali koje i dalje osoba može riješiti. Ta osoba tada mora poslati natrag ispravan odgovor.

Glavni problem kod mehanizma izazova/odgovora je taj da može generirati dodatni promet e-pošte, koji je kontraproduktivan za davatelje usluga i tvrtke koje pokušavaju smanjiti količinu generirane e-pošte. Legitimna e-pošta može također biti odbačena ako pošiljatelj ne odgovori na poruku s rješenjem (odgovor) unutar određenog vremena.

Bayesiansko filtriranje

Bayesiansko filtriranje oblik je klasificiranja teksta koje se može primijeniti na otkrivanje *spama*. Bayesianski filtar "uči" razlikovati *spam* i *ham* zapažanjem razlika između jezika koji se koristi u *spam* porukama i jezika u željenoj pošti. Na primjer, fraza "klikni ovdje" može se pojaviti u 90 od 100 *spam* poruka. Filtar dodjeljuje visoku vjerojatnost frazi "klikni ovdje" kao indikatoru *spama*. U drugu pak ruku, "Area 51" može se pojavljivati u većini UFO *junk* poruka koje nisu *spam*. U tom slučaju, filtar dodjeljuje visoku vjerojatnost da prisutnost "Area 51" indicira poruku koja nije *spam*.

S dolaskom nove poruke, filtar pregledava riječi ili fraze s najvišom vjerojatnošću u oba smjera – *spam* ili *ne-spam*. Zatim filtar proračunava novu vjerojatnost da je poruka *spam* korištenjem pojedinačnih ocjena skupljenih riječi.

Bayesiansko filtriranje privlači pažnju zbog svoje nevjerojatne stope uspješnosti otkrivanja *spama*. Bill Yerazunis, tvorac filtra pod imenom CRM114 (http://crm114.sourceforge.net), tvrdi da je točnost veća od 99,9 posto na njegovoj vlastitoj ulaznoj pošti. Paul Graham, tvorac Bayesianskog filtra, tvrdi da je stopa otkrivanja u jednom mjesecu iznosila 99,75%. On je također izvijestio osam lažnih pozitivnosti u više od 7.000 legitimnih poruka u tom razdoblju. Njegov esej, "Plan za spam"

(A Plan for Spam), detaljnije opisuje Bayesiansko filtriranje na adresi http://www.paulgraham.com/spam.html.

Bayesianski filtri najbolje funkcioniraju ako pojedinačni korisnici sami uče na svojim vlastitim *spam* i *ne-spam* porukama. Znajte da Bayesianski filtar mora redovito ponovno "učiti" da bi se prilagodio promjenama u *spamu*. Bez toga, njegova uspješnost opada. *Spameri* se upuštaju i u Bayesiansko trovanje, u kojem uključuju velike komade nasumičnog teksta u poruku, poput odlomaka iz enciklopedija, da bi pokušali progurati sadržaj poruke s ocjenom *ne-spam*.

Filtriranje reputacije

Nekoliko tvrtki sada prati IP adrese i domene i daje im ocjenu reputacije na temelju količine dobrih poruka e-pošte i količine *spam* e-pošte koju šalju. Poslužitelji za e-poštu iz bilo kojeg izvora konfigurirani su tako da blokiraju poruke e-pošte iz izvora s lošom reputacijom. To je na neki način slično crnim listama, osim što filtri reputacije mogu biti mnogo fleksibilniji. Na primjer, IP adresa ili domena mogu se ukloniti iz filtra reputacije brže, kada se njihovo ponašanje počne mijenjati.

Tvrtka pod nazivom Cloudmark oslanja se na mišljenja korisnika da bi odvojila *spam* od "hama". Ako pretplatnici Cloudmarka prime poruku koju smatraju *spamom*, oni će poruku proslijediti Cloudmarku, a onda će tvrtka za tu poruku kreirati potpis. Usluga potom ocjenjuje reputaciju korisnika zbog točnosti u odlučivanju treba li Cloudmark blokirati poruku za cijelu zajednicu. Cloudmark tvrdi da u svojoj zajednici ima više od jednog milijuna korisnika. Ako koristite Microsoft Outlook ili Outlook Express, ovu biste uslugu mogli besplatno isprobati na adresi www.cloudmark.com/safetybar/.

Drugi pokušaj filtriranja reputacije je program Bonded Sender. Tvrtke koje šalju gomile komercijalnih poruka e-pošte koje su klijenti tražili (poput biltena, financijskih izvještaja itd.) često otkrivaju da njihove poruke blokiraju *spam* filtri. Da bi pomogle u tome da legitimne komercijalne poruke prođu kroz *spam* filtre, te organizacije mogu položiti financijske obveznice kroz program Bonded Sender. Ako se neki krajnji korisnik bude žalio da je e-pošta zapravo bila nepoželjna, organizacija plaća novčanu kaznu za koju sredstva dolaze od vrijednosti obveznice. Zauzvrat, za ovo jamstvo, vlasnici *spam* filtara mogu dopustiti da poruka e-pošte sudionika Bonded Sendera zaobiđe njihove filtre. Program Bonded Sender sponzorira tvrtke IronPort, koji proizvodi poslužitelje e-pošte. Pojedinačni se korisnici ne mogu pridružiti ovom programu, ali o tome možete više saznati na adresi www.bondedsender.com.

6.5 Kako reducirati *spam*?

Postoje brojni načini koji osiguravaju da vaš poštanski sandučić ne bude zatrpan *spamom*. Ovaj odjeljak objašnjava jednostavne tehnike koje možete koristiti bez ikakvih troškova. Većina ih obuhvaća dozu zdravog razuma. Općenito, tretirajte svoju adresu e-pošte na isti način na koji tretirate druge osjetljive informacije, poput svojeg telefonskog broja. Ovi savjeti neće eliminirati *spam*, ali vam mogu pomoći da njihovu količinu zadržite u podnošljivim granicama.

Izbrišite sumnjive poruke e-pošte bez otvaranja

Moguće da *spam*, *phishing* ili prijevarne poruke otkrijete prema informacijama u adresi pošiljatelja ili u retku predmeta poruke. Sljedeći vam popis može pomoći da identificirate nepoželjnu poštu. Ako ste sumnjičavi oko neke poruke, najbolje će biti da je izbrišete bez otvaranja. Mnoge *spam* poruke koriste Web signale, koji su prije opisani, da otkriju aktivnu adresu e-pošte. Otvaranjem takve poruke, aktivirate signal i vaša e-adresa *spamerima* postaje vrjednija. Mnoge *phishing* poruke danas prenose viruse ili drugi *malware* koji može napasti vaše računalo jednostavnim otvaranjem vaše e-pošte. Zato je najbolje da sumnjive poruke izbrišete bez čitanja.

Evo nekoliko savjeta za uočavanje *spam* i *phishing* e-pošte bez otvaranja poruke:

- Adresu poruke e-pošte nikada prije niste vidjeli.
- Domena u adresi poruke dolazi iz strane zemlje s kojom niste imali nikakvog posla.
- Tekst u retku Subject ima čudan pravopis i nepoznate znakove (na primjer, V1AGR@).
- Tekst u retku Subject je nerazumljiv ili privlačan (na primjer, "Urgent!", "Important Notification!"ili "INVITATION", odnosno "HITNO!", "Važna obavijest!" ili "POZIVNICA").
- Tekst u retku Subject naznačuje neku vrstu ponude, prijedloga, rasprodaje ili poslovne transakcije.
- Tekst u retku Subject koristi "Re:" i nejasan izraz kao što je "Vaš dokument" ili "Prema razgovoru" da bi djelovalo kao odgovor na poruku koju ste vi poslali. Ne prepoznajete li adresu e-pošte ili kontekst konverzacije, tada se vjerojatno radi o triku.
- Poruka tvrdi da dolazi od banke ili neke lokacije za e-trgovinu s kojima ne poslujete.

Ne odgovarajte na *spam* ili *phishing* poruke

Ako otvorite poruku za koju se uspostavi da je *spam*, nemojte na nju odgovoriti. Odgovaranje samo informira *spamera* da je pogodio aktivnu adresu. Neke *spam* poruke tvrde i da imaju politiku poštovanja odbijanja primanja. To znači da možete odgovoriti i napisati kako ne želite primati buduće poruke. Tu se najčešće radi o triku. Ako odbijete primanje budućih poruka, *spameri* znaju da su pogodili aktivnu adresu.

U porukama kojima ne vjerujete ne klikajte na veze

Ako ste otvorili neku poruku e-pošte i dalje niste sigurni je li ozbiljna, nemojte klikati na veze u njoj. Te bi veze mogle aktivirati *malware* ili vas odvesti na lažnu Web lokaciju. Želite li ipak istražiti ponudu, zatvorite poruku, otvorite svoj Web pretraživač i ručno upišite adresu u polje URL. Mogli biste provjeriti i Web lokaciju Anti-Phishing Working Group (APWG). APWG je organizacija koja koristi najbolja iskustva iz struke za rješavanje problema u vezi s *phishing* napadima. Grupa kreira bazu podataka *phishing* poruka da bi pomogla korisnicima pri identificiranju e-poruka s namjerom prijevare. Zbirku takvih poruka možete pronaći na adresi www.antiphishing.org te klikom na vezu Phishing Archive na lijevoj strani stranice.

Čitajte izjave o privatnosti

Prije nego što počnete poslovati s nekom lokacijom za e-trgovinu, najbolje je da najprije pročitate izjavu o privatnosti kako biste saznali koje će informacije ona prikupiti (većina lokacija zahtijeva adresu e-pošte) i što će s tim informacijama učiniti. Legitimne bi tvrtke trebale pružiti jasnu vezu do izjave o privatnosti na svojoj Web lokaciji. Također bi vam trebale pružiti mogućnost da ne prihvatite isporuku nepoželjnih poruka e-pošte i zabranite tvrtki da vaše informacije prodaje drugim tvrtkama.

Ne šaljite svoju adresu e-pošte

Ako često posjećujete sobe za čavrljanje ili šaljete poruke na forume ili blogove, nemojte uključivati svoju adresu e-pošte. Također, ako imate vlastitu Web stranicu, ne prikazujte na njoj svoju adresu e-pošte. *Spameri* koriste automatizirane programe koji plaze Internetom i ubiru adrese e-pošte (uglavnom tražeći znak @).

Promijenite svoju adresu e-pošte ili koristite nekoliko adresa

Ako već želite objaviti svoju adresu e-pošte, možete je promijeniti čime ćete spriječiti automatizirane gmizavce u ubiranju vaše adrese. Dva najčešća trika je da ne pišete znak @ ni točku (johndoe at isp dot com) ili da dodate frazu poput "no spam" u adresu (janedoe@nospam.isp.com). Svaki gmizavac koji sakuplja adrese neće moći dostaviti poruku na tu adresu, a ljudi bi trebali biti dovoljno upućeni da izostave frazu iz adrese kada vam šalju poruku. (Ako se brinete da će ljudi misliti kako je "no spam" dio vaše adrese, na Web stranicu možete staviti upute.)

Međutim, mnogi *spam* programi vjerojatno će poboljšati svoje alate dovoljno da otkriju ovakve trikove, pa je druga opcija korištenje nekoliko adresa e-pošte. Na primjer, jednu adresu možete imati za svoju obitelj i prijatelje. Zatim možete kreirati dodatnu adrese koje ćete koristiti u javnosti, koje objavljujete *online* u javnosti ili ih koristite kada radite s lokacijama za koje sumnjate da vašu adresu mogu prodati ili s njome trgovati na neki drugi način.

Još jedna opcija koja vam preostaje je da odaberete adresu e-pošte koja nije očigledna. Na primjer, umjesto da koristite kombinaciju svojeg imena i prezimena (johndoe@isp.com), pokušajte koristiti kombinaciju slova i brojki ili neke fraze (na

Jedan od dobrih načina izbjegavanja *spama* je taj da imate DVIJE aktivne e-mail adrese:
1. pop3 baziranu adresu kod vašeg omiljenog ISP-a i tu adresu podesite na Outlook-u, Outlook Express-u, Eudori, ili bilo kojem e-mail klijentu na kojeg ste navikli. Tu adresu dajte samo osobama kojima vjerujete i nigdje je ne objavljujte. Biti će dobro zaštićena od *spama* i ostalih e-zala.
2. web baziranu e-mail adresu na nekoj od kvalitetnih web lokacija koje pružaju tu mogućnost (poput Yahoo-a, Lycos-a ili domaćih pružatelja usluga – a u posljednje vrijeme sve popularnija postaje usluga Gmail, kao dio Google usluga, no u trenutku pisanja ove knjige još je u *beti*). Svi ti pružatelji usluga imaju kvalitetne i moćne alate za uklanjanje *spama* i drugog smeća koje traži put do vas. To im je u interesu, jer kvalitetnim sustavom filtriranja poruka (i aktivnim antivirusnim softverom i brojnim drugim alatima) smanjuju broj proruka koje moraju usmjeriti do vas i do 90% – i stoga ih pustite da rade za vas. Takvu adresu objavljujte široj javnosti, koristite je kad pristupate *news* grupama, upisujte je kad morate dati svoje podatke da biste pristupili dodatnim sadržajima web stranica, ili kada vas neki dosadnjaković uporno traži e-adresu. Poruke takve adrese čitajte *online*, na web stranici, zaštićeni brojnim profesionalnim i dobro održavanim alatima pojedinog pružatelja usluga, gdje vaša privatnost ostaje zaštićena jer čak i prema obliku adrese vi biste podjednako lako mogli biti na sjevernom polu, usred Zagreba ili na tropskom otoku. A ukoliko se vaš web e-mail sandučić jednog dana počne puniti smećem, to znači da taj pružatelj usluga ne radi dobro svoj posao. Otvorite drugu adresu, a staru ugasite – ili jednostavno zaboravite na nju.

op.red.

primjer, j225doe@isp.com ili dontpanic@isp.com). To može spriječiti spam napade preko rječnika (iako vam može i otežati pamćenje vlastite adrese).

Dodatno, neke usluge e-pošte omogućuju vam da kreirate "privremene" adrese. Na primjer, Yahoo! Mail Plus omogućuje vam da kreirate 500 adresa na svojem Yahoo računu (ova opcija nije dostupna na besplatnom računu Yahoo! Maila). Privremene adrese možete koristiti pri radu s lokacijama za e-trgovinu, slanje poruka na oglasne ploče itd. Ako na privremenu adresu počinjete dobivati velike količine *spama*, možete jednostavno tu adresu ugasiti, pa poruke koje je koriste više neće stizati. Sa svojim ISP-om ili davateljem Web poštanskih usluga možete provjeriti nude li slične opcije.'

Ne kupujte ništa od *spamera*

Kad bi svi na svijetu poštivali ovu uputu, *spam* bi prestao postojati. Na žalost, ima dovoljan broj ljudi koji su ili lakovjerni ili dovoljno znatiželjni da kupuju nešto što *spam* nudi. Zbog toga ćemo se vjerojatno morati oslanjati na tehnološka rješenja dok ne dođe dan kad će se glupost moći ispraviti kirurškim putem.

Izvijestite o *spamu* i *phishingu*

Spam ili *phishing* poruke možete prijaviti raznim organizacijama uključujući svojeg davatelja Internet usluga, vladu i *anti-spam/anti-phishing* organizacije. Prijavljivanjem *spama* pomažete svojem ISP-u da poboljša sposobnosti otkrivanja *spama*; vaša prijava može pružiti i dodatni dokaz, ako vaš ISP odluči poduzeti zakonske korake protiv spamera. Pitajte svojeg ISP-a koje korake trebate vi poduzeti za prijavljivanje *spama*. Besplatna usluga pod nazivom SpamCop može za vas prijaviti *spam* i dodati izvor *spama* na popis za blokiranje. Morate se registrirati na Web lokaciji (www.spamcop.net), a vaša je adresa e-pošte potrebna da bi se moglo prikazati cijelo zaglavlje poruke (a ne samo zaglavlja To: i From:). Pogledajte FAQ stranicu Web lokacije tvrtke kod koje imate račun e-pošte da biste saznali kako otkriti cijela zaglavlja poruka.

Spam i *phishing* e-poštu možete prijaviti i FTC-u. FTC skuplja *spam* e-poštu da bi provodila zakonske korake protiv *spamera*. *Spam* e-poštu možete poslati na adresu spam@uce.gov. (UCE je kratica za Unsolicited Commercial E-mail, Nepoželjna komercijalna e-pošta, op. prev., pristojniji izraz za *spam*.)

Na kraju, *phishing* e-poštu možete poslati na Anti-Phishing Working Group. APWG preferira da ljudi ne prosljeđuju *phishing* poruke. Umjesto toga trebali biste otvoriti novu poruku i adresirati je na reportphishing@antiphishing.org, te ulijepiti *phishing* poruku u novu poruku i poslati je.

6.6 *Anti-spam* alati

Na tehnološkoj razini, rat sa *spamom* najprije su vodili davatelji usluga i administratori korporativnih ili osobnih poslužitelja e-pošte. To je korisnicima uglavnom nevidljivo (osim ako zalutali *spam* nađe put do vašeg poštanskog sandučića). Većina davatelja usluga dopušta klijentima neki stupanj prilagođavanja. Na primjer, AOL svojim pretplatnicima omogućuje kreiranje vlastitih crnih lista, korištenje filtriranja po ključnoj riječi i blokiranje slika uključenih u poruke nepoznatih pošiljatelja. Yahoo! korisnicima omogućuje kreiranje crnih lista i blokiranje slika i Web signala. Earthlink pak omogućuje korisnicima blokiranje svake poruke pošiljatelja koji se ne nalazi u njihovim adresarima (ekstreman oblik bijelih lista).

Softver je dostupan i za korisnike koji žele primijeniti dodatne *spam* kontrole na svojim kućnim računalima. Tablica 6.1 prikazuje nekoliko opcija. Jednostavno pretraživanje Web-a prema riječima "anti-spam software" ili "spam filters" usmjerit će vas na znatno veći izbor. Računalni časopisi i *online* Web recenzije

Tablica 6.1

Odabrani Anti-spam proizvodi

Proizvod	Proizvođač	Web lokacija	Značajke
Anti-Spam Personal	Kaspersky Lab	www.kaspersky.com	Analizira *spam* po karakterističnim atributima, koristi RBL (*realtime black list*), pretra; uje po tipičnim riječima i frazama, ima grafičku analizu *spama* u slikama, lokalne crne i bijele liste koje korisnik mo; e sam dodatno editirati; baza podataka lista se osvje; ava svaka dva sata.
Cloudmark SafetyBar 4.0	Cloudmark	www.cloudmark.com	Definira *spam* na temelju povratih informacija više od milijuna korisnika. Za Outlook i Outlook Express.
MailFrontier Desktop	MailFrontier	www.mailfrontier.com	Crne liste, bijele liste, otkrivanje *phishinga* i prijevara, povratne informacije korisnika, opcije izazov/odgovor. Za Outlook i Outlook Express, Hotmail i MSN.

Proizvod	Proizvođač	Web lokacija	Značajke
Norton AntiSpam	Symantec	www.symantec.com	Crne liste, bijele liste (sinkroniziranje s adresarima Outlooka, Outlook Expressa ili Eudore), filtriranje *spama* iz Yahoo! Web pošte, može blokirati e-poštu na stranim jezicima.
OnlyMyEmail Personal	OnlyMyEmail	www.onlymyemail.com	Temeljen na usluzi. Višestruki analitički mehanizmi, crne liste i bijele liste. Za Outlook, Outlook Express i Web poštu.
Panda Platinum Internet Security 2005	Panda Software	www.pandasoftware.com	Analitički mehanizam, bijele liste, otkrivanje *phishinga*. Za Outlook i Outlook Express.
PC-cillin Internet Security	Trend Micro	www.trendmicro.com	Filtrira *spam* za Outlook Express, AOL, Yahoo!, MSN Hotmail i Eudoru.
Spam Filter Expres	ANVSOFT	www.spam-filter-express.com	Bayesiansko filtriranje, crne liste, bijele liste. Za Outlook i Outlook Express.
SpamKiller	McAfee	www.mcafee.com	Uključuje crne liste, bijele liste, potpise *spama*, Bayesiansko filtriranje, filtriranje slika i poruka na stranom jeziku.
ZoneAlarm Security Suite	Zone Labs	www.zonelabs.com	Preusmjerava *spam* u tri mape: sumnjiva pošta, *junk* pošta, i prijevarna pošta.

anti-spam proizvoda dostupne su i u *PC Magazineu* (www.pcmagazine.com), *PC Worldu* (www.pcworld.com), CNET-u (www.cnet.com) te domaćim časopisima *Bug* (www.bug.hr), *Vidi* (www.vidi.hr), *PC Chip* (www.pcchip.hr) i drugima. Od sredine 2005. godine cijene se kreću u rasponu od 29,95 do 39,95 američkih dolara za samostalan *anti-spam* softver te od 49,95 do 79,95 dolara za sigurnosne programske pakete koje sadrže *anti-spam* i drugi važan softver uključujući anti-virus, *anti-spyware* i vatrozid.

6.7 Popis za provjeru

Ovaj je popis brzi referentni vodič za gradivo izneseno u ovom poglavlju.

Učinite

- Izbrišite sumnjive poruke bez otvaranja.
- Čitajte izjave o privatnosti.
- Čuvajte svoju adresu e-pošte koliko je moguće više privatnom.
- Prijavite *spam* i *phishing* FTC-u i Anti-Phishing Working Groupu.

Nemojte učiniti

- Nemojte klikati veze unutar sumnjivih poruka e-pošte.
- Nemojte svoju adresu e-pošte objavljivati *online*.
- Nemojte kupovati išta od *spamera*.
- Nedajte da vas zavedu alarmantne poruke koje zahtijevaju trenutnu akciju.

6.8 Korisni izvori

Ovaj odjeljak predstavlja dodatne izvore koji će vam pomoći da više naučite.

Spamroll je *blog* o svim *spamerskim* temama. On obuhvaća vijesti iz svijeta *spama*, pruža informacije o *spamu* i *phishingu* i sadrži arhivu *spam* poruka. Nalazi se na adresi at www.spamroll.com.

Možete upotrijebiti SpamCop da vam pomogne prilikom prijavljivanja *spama* svojem ISP-u. SpamCop također održava crne liste za ISP-ove i administratore e-pošte. Nalazi se na adresi www.spamcop.net.

David Sorkin prati zakonodavstvo vezano uz *spam* za državne i federalne zakone, kao i za međunarodne zakone, na adresi www.spamlaws.com.

FTC-ova Web lokaciji na adresi http://www.ftc.gov/bcp/conline/edcams/spam/index.html. uključuje i savjete kako spriječiti da *spam* zatrpava vaš poštanski sandučić.

Abuse.net prati informacije o *spamerima* i *anti-spam* tehnikama. Stranica na adresi http://spam.abuse.net/userhelp/ ima mnogo korisnih veza do savjeta i alata za koješta, uključujući filtriranje i blokiranje *spama*, skrivanje adrese e-pošte, izvore privremenih adresa e-pošte, načine praćenja *spam* poruka i načine prijavljivanja takvih poruka ISP-ima.

7. poglavlje

Osiguravanje Windowsa

Milijuni računala diljem svijeta koriste Windows operativni sustav i Microsoft aplikacije. Postoje mnoge teorije koje objašnjavaju prevlast Microsofta: mudar marketing; dobri programeri; volja tvrtke da licencira svoj softver bilo kojem proizvođaču PC-a; Appleovo inzistiranje da radi upravo suprotno, čime velik dio tržišta prepušta Microsoftu; monopolistička rafiniranost. Iz bilo kojeg od ovih razloga (i u svakom postoji dio istine), Microsoft ima najdominantniji operativni sustav i programski paket na svijetu.

Ova je nadmoć dobra za dvije grupe ljudi: Microsoftove dioničare i ljude koji kreiraju *malware*. Krajolik kojim dominira jedan operativni sustav predstavlja plodno okruženje za viruse, crve, trojanske konje i *spyware*. Svaki softver ima određene pukotine, a svi se operativni sustavi i aplikacijske platforme mogu zlorabiti. No, kada jedna obitelj softvera dominira, pisci *malwarea* koji žele imati najveći učinak ciljaju i najveću metu. Logotip Windowsa može se zamijeniti i crnim krugom u sredini streljačke mete.

A ako još uzmete u obzir koliko je jak postao Internet kao mehanizam za trgovinu, napadanje najpopularnijih softverskih platformi vjerojatnije da će dati bolji prinos. Ozloglašenog su pljačkaša banaka Williea Suttona pitali "Zašto pljačkate banke?". Njegov je odgovor glasio: "Jer je u njima novac." Baza Microsoftovog koda je najveća banka, pa stoga privlači pažnju ljudi koji se pokušavaju provući kroz razbijene prozore, rupe na krovu ili jednostavno upasti na prednja vrata s

pištoljima. Kriminalci vam dolaze s raznoraznim pristupima, od kojih se većina vrti oko zlorabljenja Windows operativnog sustava ili Web pretraživača Internet Explorera (IE).

Je li zaista Microsoft pod paljbom? Test koji je proveo *USA Today*[1] pokazao je da je u toku dva tjedna dnevno provedeno 8.177 pokušaja provaljivanja u računala na kojima se izvodio Windows XP Service Pack 1 (SP1) s DSL Internet vezom. To je alarmantno velik broj, pogotovo uzmemo li u obzir činjenicu da je test izuzeo dva značajna smjera napada: e-poštu i Web pretraživanje.

Dobra je vijest ta da je samo jedan od devet pokušaja napada zapravo uspio, a računalo nije imalo najnovije zakrpe i sigurnosni softver. Nasuprot tome, stroj na kojem se izvodi Windows XP s vatrozidom ZoneAlarm pretrpjelo je dnevno 50 napada, ali ni jedan nije uspio. (Test je obuhvaćao i računala na kojima se izvodi Mac OS X i Linspire, korisnički orijentirani Linux-temeljeni operativni sustav iz Microtela. OS X računalo pretrpjelo je gotovo isto toliko pokušaja napada kao i Windows računalo na kojem se izvodio SP1 (iako ni jedan pokušaj nije uspio). Linspire računalo napadnuto je nešto manje od 800 puta, bez uspješne provale.

Najjednostavniji savjet koji vam mogu dati je da razmotrite korištenje nekog drugog operativnog sustava kada sljedeći put kupujete računalo. Stari korisnici operativnih sustava tvrde da je Macintosh računala lakše osigurati jer se radi o superiornim proizvodima. Je li to zaista tako, ja doista ne mogu reći. Ono što mogu reći je to da je većina *malwarea* napisana za Microsoft platformu, pa je alternativni operativni sustav manje otvoren za uspješne napade.

Koristite li Windows računalo, temeljno je da ga osigurate. Prva stvar koju trebate napraviti je instalirati vatrozid i postaviti ga u način rada *stealth*. Sljedeća stvar je osigurati da imate sve najnovije zakrpe za Windows operativni sustav i sve aplikacije koje koristite (uključujući i one koji nisu Microsoftove). Na kraju, poduzmite korake da biste osigurali Internet Explorer. Trebali biste također razmisliti o alternativnom pretraživaču, kao što je Firefox ili Opera. Iako ni ti pretraživači nisu potpuno otporni na napade, oni izbjegavaju neke od sigurnosnih problema koji su pridruženi s IE-om, i manje su mete koje ne privlače toliku pažnju kriminalaca (iako bi se ovo moglo brzo promijeniti s porastom popularnosti Firefoxa).

---

1 "Unprotected PCs Can Be Hijacked in Minutes," autora Byrona Acohidoa i Jona Swartza, *USA Today*, 29. studeni 2004.

Ovo poglavlje opisuje specifičnosti zaštite Windows XP Service Packa 2 (SP2). Windows XP SP2 je najnovija verzija Microsoft operativnog sustava za korisnike i jedina koju Microsoft trenutno podržava. Razmotrit ćemo i kako IE učiniti sigurnijim te mjesta na kojima se mogu pronaći alternativni pretraživači.

7.1 Windows XP Service Pack 2

Microsoft je u potpunosti svjestan da su njegovi proizvodi pod stalnim napadima. Tvrtka je također svjesna i toga da dugoročno riskira rušenje vlastite reputacije (ako ne i sebe same) bude li Windows nastavio biti hrana za razni proždrljivi *malware* i neprimjetne provalnike. Windows XP sa Service Pack 2 dio je zajedničkog truda Microsofta da poboljša sigurnosne sposobnosti Windows platforme izvlačenjem iz usta crva. Nadogradnja SP2 besplatno je dostupna, uz pretpostavku da ste već kupili XP. Koristite li stariju verziju Windowsa, trebat ćete kupiti novi operativni sustav koji bi se trebao isporučivati sa SP2.

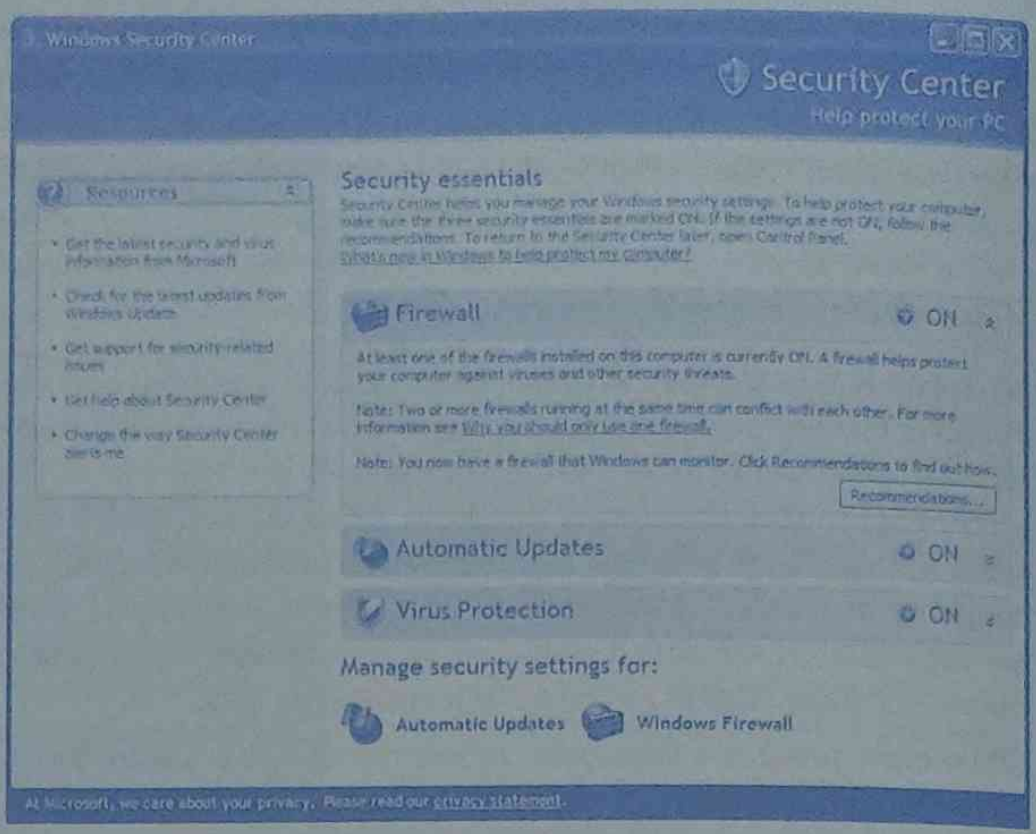
SP2 možete preuzeti s Windows Update (ali se radi o velikoj datoteci, pa odvojite dovoljno vremena, osobito ako koristite *dial-up* vezu). Sve potrebne podatke o SP2 potražite na adresi www.microsoft.com/windowsxp/sp2/default.mspx ili na www.microsoft.com/croatia (upišite samo www.microsoft.hr).

Sljedeći odjeljak daje pregled novosti u zakrpi SP2 – naročito onih koji se odnose na mehanizme zaštite ugrađene u softver.

Windows Security Center

Glavno poboljšanje u zakrpi SP2 je Security Center, koji postavlja nekoliko vrlo važnih kontrola na jednu lokaciju. Iz Security Centera možete nadzirati status antivirusnog softvera, upravljati Windows Firewallom i postaviti automatsko ažuriranje softvera.

Da biste pristupili Security Centeru, kliknite gumb Start, odaberite Control Panel i Security Center (to je ikona štita). Kada se otvori prozor Security Center vidjet ćete tri glavna okna: Firewall, Automatic Updates i Virus Protection (pogledajte sliku 7.1). Svako okno ima statusno svjetlo koje indicira je li pridružena funkcija uključena. Svako ima gumb koji aktivira mali padajući ekran s detaljnijim informacijama o pojedinim funkcijama.



Slika 7.1 Windows Security Center

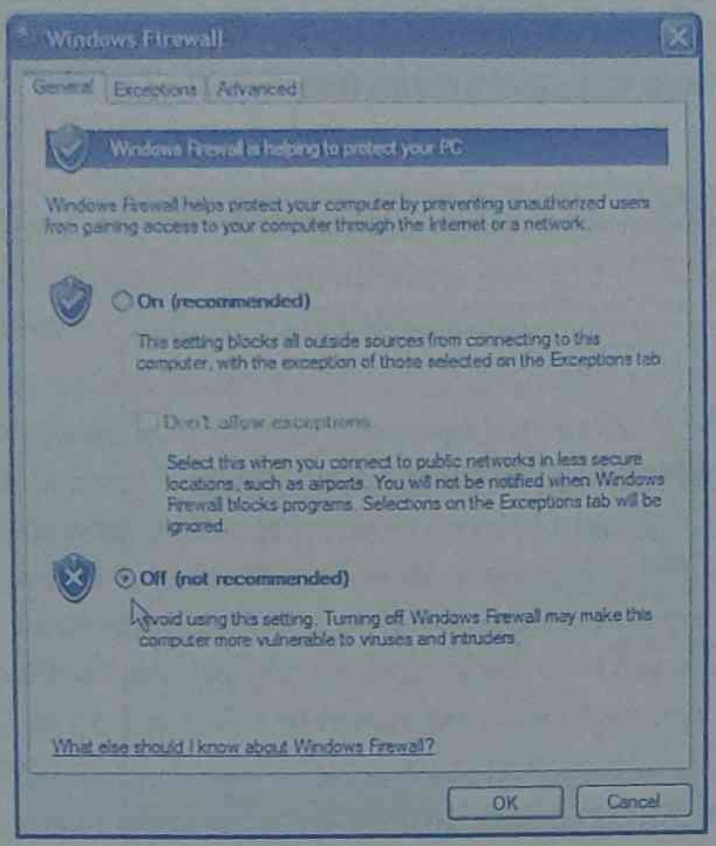
Ispod okna nalaze se dvije ikone: Automatic Updates i Windows Firewall. Da biste aktivirali odnosnu funkciju i promijenili postavke možete kliknuti te ikone. Prozor Resources u gornjem lijevom kutu nudi veze do dodatnih informacija o sigurnosti.

Počnimo s ikonom Windows Firewall. Windows XP SP2 uključuje osnovni vatrozid koji sprječava da se drugi strojevi na Internetu povežu s vašim računalom, osim ako se vi na njih ne spojite prvi. Windows Firewall je prema osnovnoj postavki uključen, pa ako njega koristite kao jedini vatrozid, on je već aktiviran.

Kao što smo objasnili u 3. poglavlju "Vatrozidovi", iako je Windows Firewall odličan u blokiranju nepoželjnih veza koje s Interneta pokušavaju uspostaviti s vašim računalom, on neće poduzeti ništa u vezi s crvima ili virusima koji dolaze na vaš stroj i pokušavaju uspostaviti veze s vašeg računala do Interneta. Zato Windows Firewall radi samo polovicu posla (iako važniju polovicu). Pravi vatrozid trebao bi nadzirati pokušaje vašeg računala da uspostavi veze s Internetom. To je zbog toga što *malware* i *spyware* često otvaraju veze s Internetom da bi povratno izvještavali kontrolni poslužitelj, dobivali ažurirane upute i pokretali napade na

nove mete. Zato vas vatrozid koji nadzire izlaznu komunikaciju može upozoriti ako neki sumnjivi program odjednom želi razgovarati s nekim na Internetu.

3. poglavlje, "Vatrozidovi", daje popis brojnih vatrozidova koji nude obje funkcije, pa vam preporučujemo da upotrijebite jedan od tih vatrozidova i instalirate ga na svoje računalo. Ako koristite još neki vatrozid, tada biste najprije trebali onemogućiti Windows Firewall. Nećete biti dvostruko zaštićeni ako koristite vatrozid nezavisnog proizvođača istodobno s Windows Firewallom. Zapravo bi istodobno izvođenje dva ili više vatrozida na jednom računalo moglo prekinuti korištenje Interneta. Da biste onemogućili Windows Firewall, kliknite ikonu Windows Firewall na dnu stranice Security Center. Otvorit će se iskočni prozor prikazan na slici 7.2; kliknite gumb Off. Neki vatrozidovi nezavisnih proizvođača tijekom instaliranja sami isključuju Windows Firewall.

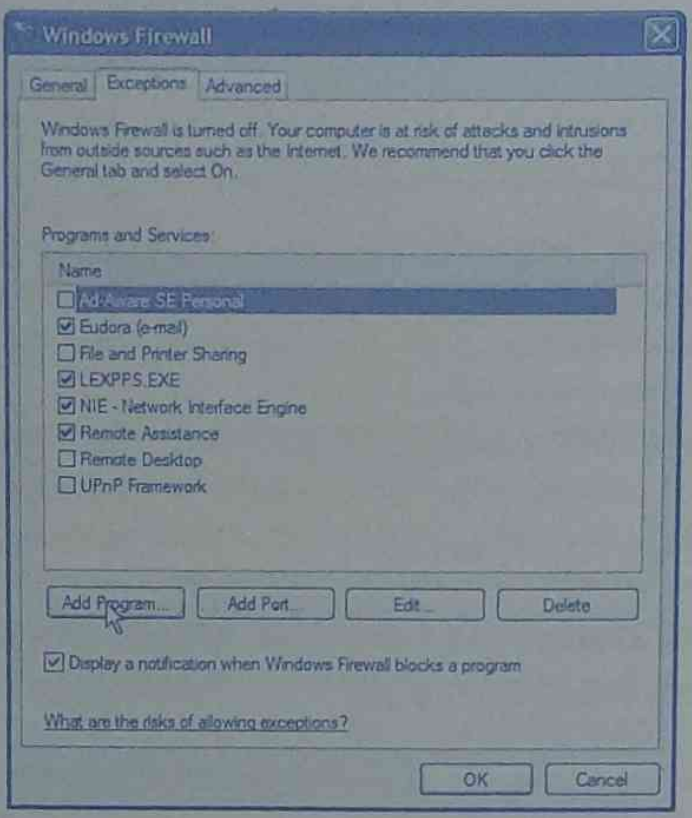


Slika 7.2 Stranica Windows Firewall

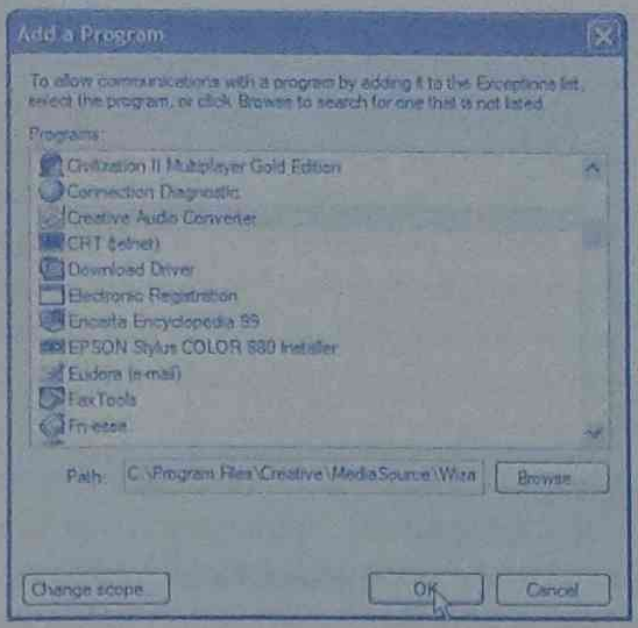
Čak i ako isključite Windows Firewall, Security Center će vas i dalje obavještavati ako pronađe neki vatrozid nezavisnog proizvođača i ako je on uključen. Microsoft bi trebao biti u stanju pronaći većinu poznatih vatrozidova.

Konfiguriranje Windows Firewalla

Ako koristite Windows Firewall, ne biste se trebali gnjaviti s velikim brojem konfiguracijskih problema za glavne zadatke kao što je surfanje Webom te slanje i primanje e-pošte. Međutim, trebali biste biti svjesni nekih osnovnih konfiguracijskih pitanja. Vatrozid može spriječiti neke programe, poput igara i softvera za dopisivanje u realnom vremenu od otvaranja veza s Internetom. Ovo možete promijeniti klikom ikone Windows Firewall na dnu stranice Security Center. Otvara se prozor prikazan na slici 7.2. Kliknite jahač Exceptions. Vidjet ćete popis programa pod nazivom Programs and Services prikazan na slici 7.3. Pregledajte popis da biste vidjeli je li program za koji želite da vam dopusti komunikaciju s Internetom na njemu. Ako nije kliknite gumb Add Program pa pregledajte popis Programs kao što je prikazano na slici 7.4. Odaberite program i kliknite OK. To premješta odabrani program na popis Programs and Services kao što je prikazano na slici 7.3. Neka dodani program bude potvrđen pa kliknite OK. Windows Firewall će sada programu dopustiti pristup Internetu.



Slika 7.3 Kartica Exceptions Windows Firewalla

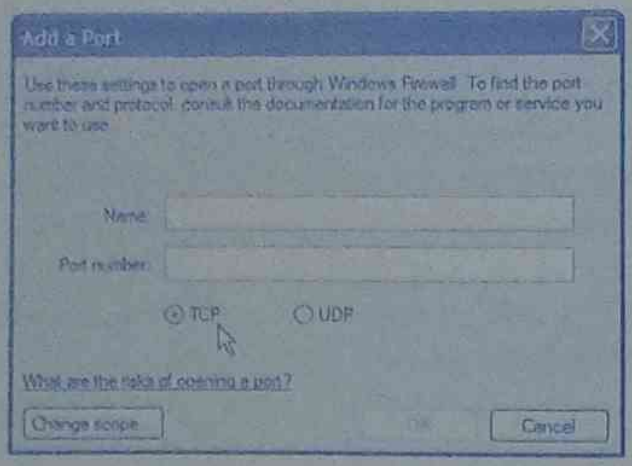


Slika 7.4 Dijaloški okvir Add a Program

Broj izuzetaka trebali biste održavati što je moguće manjim. Što više izuzetaka kreirate, više ćete 'pukotina' otvoriti u vatrozidu, a to će povećati šansu da neki provalnik ili *malware* pristupi vašem računalu.

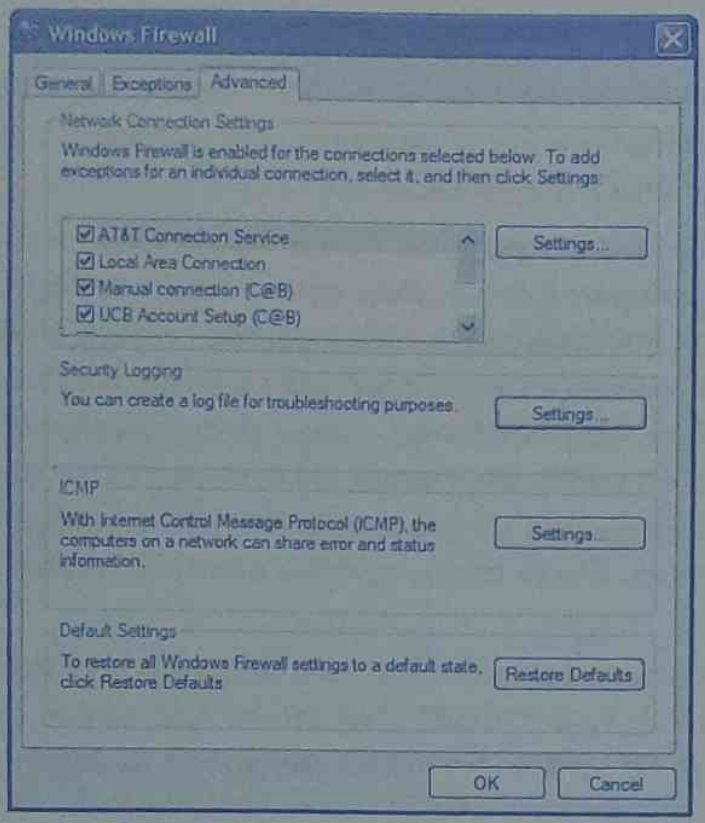
Popisu izuzetaka možete dodati i portove. Port je ulaz u vaše računalo koji određenim programima ili uslugama omogućuje komunikaciju s vašim računalom. Na primjer, Web promet koristi port 80. Vaše računalo zna koji portovi trebaju biti otvoreni za uobičajene aplikacije poput Interneta i e-pošte. Neki programi koriste razne portove (*online* igre, VoIP telefonija, sustav za dopisivanje u realnom vremenu dobri su primjeri takvih programa), pa ćete stoga morati ručno otvoriti te portove da biste omogućili rad tih programa. Ono što vrijedi i za programe, to također vrijedi i za portove. Što je manje portova otvoreno, manje je rupa u vašem vatrozidu.

Ako znate koji port ili portove želite otvoriti, kliknite gumb Add Port... na ekranu koji je prikazan na slici 7.3. To će otvoriti novi prozor Add a Port, prikazan na slici 7.5. On vam omogućuje da upišete ime i broj porta.



Slika 7.5 Dijaloški okvir Add a Port

Da biste dodatno konfigurirali vatrozid upotrijebite karticu Advanced prikazanu na slici 7.6. Taj prozor ima četiri sekcije: Network Connection Settings, Security Logging, ICMP i Default Settings.



Slika 7.6 Kartica Advanced Windows Firewalla

Ispod Network Connection Settings trebali biste vidjeti vezu sa svojim ISP-om.

Ispod Security Logging možete kreirati sigurnosni dnevnik da biste vidjeli veze koje su dopuštene ili odbijene. Ti dnevnici nemaju nekog smisla ako baš nemate iskustva s radom u mreži, ali ako vas zanima kako izgleda neka IP adresa, koje portove koristi vaše računalo i koje su IP adrese lokacija na koje se spajate, tada pogledajte taj dnevnik. (Ogledni primjer dnevnika nalazi se na slici 3.2 u 3. poglavlju.) Windows XP SP2 ima unaprijed zadano odredište za spremanje dnevnika (C:WINDOWS/pfirewall), ali datoteku može spremati na bilo koje drugo mjesto. Zapamtite da ova funkcija bilježenja radi samo za Windows Firewall. Ako koristite vatrozid nekog nezavisnog proizvođača, on će kreirati svoje dnevnike, koje biste trebali pronaći preko njihovog korisničkog sučelja.

Format dnevnika uključuje datum i vrijeme svake akcije, opis akcije (na primjer, otvaranje veze s drugim računalom), protokol (TCP itd.), izvorišne i odredišne IP adrese, izvorišni (to ste vi) i odredišni port te informacije o pojedinačnim paketima koji čine Internet komunikaciju. Detalje o portovima, protokolima i Internet komunikaciji naći ćete u 3. poglavlju.

Sekcija ICMP na kartici Advanced računalu omogućuje da šalje i prima Internet Control Message Protocol (ICMP) poruke. ICMP je korisna za administratore računalnih mreža zbog informacija o zdravlju sustava, ali se kućni korisnici ne trebaju zamarati s ICMP porukama. Zapravo, neki napadači koriste ICMP poruke da provjere hoće li računalo odgovoriti. Zbog toga je najbolje da onemogućite sve ICMP poruke.

Konačno, sekcija Default Settings je mjesto na kojem ćete moći početi, preskačući sve ovo što vam se čini kompliciranim s obzirom na vaše iskustvo pri radu s Internetom. Jednostavno kliknite gumb Restore Defaults da biste Windows Firewall vratili na originalne postavke. Zapamtite da se klikom gumba Restore Defaults brišu sve promjene postavki vatrozida koje ste proveli uključujući programe koje ste dopustili, portove koje ste otvorili itd.

Zaštita od virusa

Windows XP SP2 nema ugrađenu zaštitu od virusa, ali vas može obavijestiti o antivirusnom programu nezavisnog proizvođača te o tome ima li program ažurirane sve najnovije antivirusne zaštite. No, zapamtite da Microsoft ne nadzire svaki AV softver. Na adresi www.microsoft.com/security/partners/antivirus.asp možete provjeriti podržava li Microsoft vaš AV softver. Djelomičan popis podržanih AV programa uključuje Symantec, Trend Micro, Computer Associates, GFI, F-Secure, Sophos, Kaspersky, McAfee i Panda Software.

Iako Microsoft ne pruža korisnički antivirusni softver (premda će se ovo vrlo vjerojatno promijeniti, moguće u sljedećoj verziji Microsoftovog operativnog sustava), on ima besplatni pomoćni program koji provjerava postoji li na računalu uobičajeni *malware*. Alat Malicious Software Removal Tool skenira vaše računalo prema popisu zlonamjernog softvera i uklanja svaki koji pronađe. Dok sam pisao ovo poglavlje, taj je alat otkrio 20 obitelji (uključujući varijante) poznatih crva i virusa. Ako imate antivirusni softver nezavisnog proizvođača, tada biste već trebali biti zaštićeni od tih obitelji *malwarea*. No, ako ste znatiželjni, neće smetati da preuzmete alat s adrese www.microsoft.com/security/malwareremove i vidite što će pronaći.

Ako ste uključili opciju Automatic Updates (pogledajte odjeljak "Uključivanje opcije Automatic Updates"), alat se automatski učitava i izvodi. Kada alat završi izvođenje, sam sebe briše. Imajte na umu da ovaj alat nije nadomjestak za antivirusni program. Iako može ukloniti uobičajene oblike *malwarea*, on neće spriječiti da *malware* dođe na vaše računalo. Nasuprot njemu, ažurirani antivirusni proizvod može otkriti i blokirati *malware* prije nego što se instalira na vaše računalo. Uz to, Malicious Software Removal Tool otkriva i uklanja samo mali podskup *malwarea* koji može otkriti i ukloniti antivirusni program.

Zaštita od prelijevanja međumemorije

SP2 pomaže u zaštiti Windows operativnog sustava i nekih komunikacijskih protokola od tehnike napada koja se naziva prelijevanje međumemorije *(buffer overflow)*. Pomoću te tehnike, maliciozni program pokušava injektirati više koda u područje memorije računala, koje se naziva međumemorija, od onoga što to područje može prihvatiti. Višak koda, koji uglavnom sadrži upute za preuzimanje kontrole nad računalom, teče u drugo područje memorije računala i izvodi se. Automatizirani crvi uglavnom se oslanjaju na prelijevanja međumemorije. Većina računalnih operativnih sustava i aplikacija osjetljiva je na ovu vrstu napada. SP2 ne otklanja prijetnju od prelijevanja međumemorije, ali poboljšava otpornost Windowsa.

7.2 Utorci zakrpa

Svaki je softver u stalnom razvojnom procesu; ne postoji točka u vremenu u kojoj je softver dovršen. Ponekad je to zbog toga što proizvođači izdaju sljedeću verziju softvera koja sadrži nove značajke i osobine. Međutim, između specifičnih verzija,

proizvođači softvera izdaju i zakrpe. Te su zakrpe dijelovi softvera koji ispravljaju probleme u programu. Neki od tih problema su funkcionalne pogreške, bugovi, koji narušavaju normalan rad softvera. Na primjer, softverski bug može prouzrokovati da vaš kalkulator na ekranu prikaže kako je 2+2 jednako 5.

Postoji i posebna kategorija buga koja se naziva *ranjivost*. Ranjivost je pukotina ili slabost u softveru koja se može iskoristiti da računalo učini nešto što vlasnik računala ne želi. Mnogi crvi koji plaze Internetom primjeri su *malwarea* koji je dizajniran da iskorištava ranjivost softvera. Ponekad tu ranjivost otkriva sam proizvođač. Vjerojatnije je da će je prije otkriti neki istraživač izvan tvrtke. Mnoge tvrtke zarađuju na poslovima otkrivanja ranjivosti softvera. Tri najpoznatije takve tvrtke su Secunia, eEye i X-Force (koja je ogranak za istraživanje tvrtke za sigurnost pod nazivom Internet Security Systems). Te tvrtke za istraživanje dobivaju publicitet zbog svojih uspjeha u otkrivanju ranjivosti i poput novina pokušavaju nadmašiti jedna drugu, pa se zato trude da budu korak ispred svojih konkurenata.

Kada legitimna tvrtka za istraživanje otkrije ranjivost nekog softvera, pravilo je da potom kontaktira proizvođača tog softvera. Tvrtke za istraživanje uglavnom se slažu da proizvođaču daju neki vremenski okvir (recimo 30 dana, ali taj rok može znatno varirati) unutar kojeg proizvođač mora potvrditi da postoji ranjivost i za to kreirati zakrpu. Kada je zakrpa spremna, istraživač i proizvođač objave u javnosti o kojoj se ranjivosti radi kako bi korisnici mogli preuzeti zakrpu.

Na žalost, ne drže se svi gore navedenog pravila. Sumnjivi istraživači mogu otkriti ranjivosti i ne obavijestiti proizvođača softvera. Otkrivene ranjivosti mogu zadržati za sebe i iskorištavati ih ili prodati informacije drugim zainteresiranim stranama. U nekim slučajevima objave u javnosti pukotinu, tako da i proizvođač i napadači istodobno za nju saznaju. U tom slučaju počinje utrka jer se proizvođač žuri u kreiranje zakrpe, a napadači se žure iskoristiti pukotinu dok za nju ne postoji zaštita.

Da bi stvari bile gore, pisci *malwarea* objavljuju napadačke alate u sve bržem ritmu. Na primjer, u listopadu 2000. godine Microsoft je objavio zakrpu za pukotinu u svojem softveru za poslužitelje. Skoro godinu dana kasnije pojavio se crv Nimda koji je napao tu pukotinu. Nasuprot tome, u travnju 2004. godine Microsoft je objavio još jednu zakrpu za svoj softver za poslužitelje – 17 dana kasnije na scenu je stupio crv Sasser.

Drugi problem sa zakrpama su ljudi koji ih ne instaliraju čak i kada su one dostupne. Iako je zakrpa bila dostupna 336 dana prije nego što se crv Nimda pojavio, mnogo ljudi nije instaliralo zakrpu, pa je Nimda pronašao dovoljno ranjivih strojeva koje je trebao za opsežan napad.

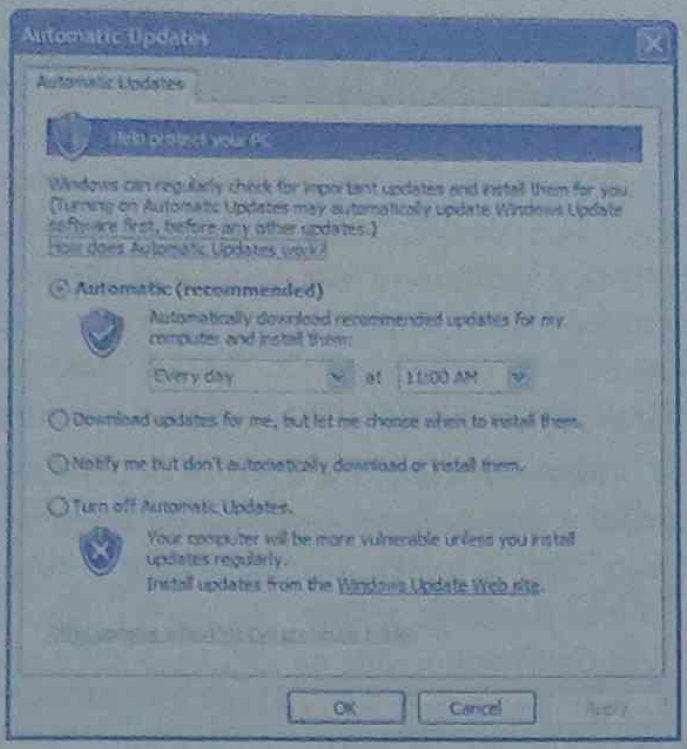
Microsoft je prije zakrpe objavljivao bez nekog vremenskog rasporeda. No, kako su se ranjivosti povećavale, tvrtka je odlučila odrediti rokove za objavljivanje zakrpa. Sada Microsoft objavljuje najnoviju verziju ažuriranog softvera svakog drugog utorka u mjesecu. Microsoft također ističe zakrpe koje rješavaju kritične pukotine. Kritične su pukotine uglavnom one koje udaljenom napadaču mogu pružiti kontrolu nad računalom ili mu na drugi način omogućiti da učini veliku štetu. Patch Tuesdays (utorci zakrpi) često obuhvaćaju barem jednu kritičnu pukotinu po seriji. Microsoft naravno izdaje hitne zakrpe izvan za to predviđenog vremena, ako je pukotina vrlo opasna.

Windows XP SP2 uključuje mogućnost automatskog ažuriranja. Svoje računalo možete konfigurirati tako da redovito posjećuje Microsoftovu Web lokaciju i provjerava postojanje novih zakrpa. Kućnim se korisnicima vrlo toplo preporučuje da uključe opcije Automatic Updates jer, kao što smo već spomenuli, napadači mogu izdati alat za napad unutar nekoliko dana ili tjedana od objave pukotine. Automatskim ažuriranjem svojeg sustava moći ćete uživati u trenutnoj zaštiti od nadolazećih napada. Druga korisna stvar je ta da nećete morati pamtiti kako svaki mjesec trebate posjećivati Microsoftovu Web lokaciju da biste preuzeli najnovije i najvažnije ispravke. Napokon, automatska je usluga praktična jer obuhvaća sve zakrpe za široku paletu Microsoftovih proizvoda, uključujući Windows operativni sustav, Internet Explorer i ostale popularne aplikacije. Zato, ako se primjerice u Windows Media Playeru otkrije ranjivost, nećete trebati posjetiti posebnu Web lokaciju da preuzmete zakrpu.

Uključivanje opcije Automatic Updates

Da biste uključili opciju Automatic Updates, kliknite ikonu Automatic Updates na dnu ekrana Security Center kao što je prikazano na slici 7.1. To otvara manji prozor pod nazivom Automatic Updates, koji vam omogućuje da odaberete svoje postavke (slika 7.7).

Možete odabrati da se ažuriranja automatski preuzimaju i instaliraju (što je Microsoftova preporučena postavka) ili možete odabrati vremenske intervale u kojima će se odvijati ažuriranje. Ako odaberete vrijeme kada je vaše računalo obično isključeno, ažuriranja će se instalirati sljedeći put kada uključite računalo. Da biste bili sigurni, ja vam preporučujem da odaberete vrijeme kada ste obično *online* čime osiguravate preuzimanje ažuriranja.



Slika 7.7 Dijaloški okvir Automatic Updates

Možete odabrati i to da se ažuriranja automatski preuzimaju ali da se instaliraju na vaš zahtjev, ili možete odabrati da budete obaviješteni o novim dostupnim ažuriranjima bez njihovog automatskog preuzimanja i instaliranja. Opciju Automatic Updates možete i isključiti.

Da biste bili sigurni kako imate sve potrebne ažurirane verzije posjetite adresu http://windowsupdate.microsoft.com. (Da biste pristupili ovoj lokaciji morate imati Internet Explorer verziju 5 ili noviju – s Firefoxom neće raditi.) Kada stignete na lokaciju, Microsoft daje dva izbora: Express Install, koji na vaš stroj kopira samo kritične i sigurnosne ažurirane verzije i Custom Install, koji vam dopušta da s popisa odaberete ažuriranja koja želite.

7.3 Osiguravanje Internet Explorera

Baš kao što je Windows najrasprostranjeniji operativni sustav na svijetu tako je i Internet Explorer najkorišteniji Internet pretraživač. Ova situacija predstavlja poznati problem: zločesti dečki povećavaju svoje šanse za preuzimanje kontrole nad vašim računalom ili za instaliranje softvera bez vašeg dopuštenja napadajući najrašireniji pretraživač.

Sigurnost Internet Explorera

Napadači mogu manipulirati Internet Explorerom na nekoliko načina. Jedan je iskorištavanje ranjivosti softvera. Na primjer, u lipnju 2004. godine pojavio se trojanski konj pod imenom Download.ject. Taj je napad iskoristio pukotine u softveru Internet Information Servera (IIS, Microsoftova Web poslužiteljska platforma) i Internet Explorera. Zlonamjerni kod najprije je učitan na ranjive Web poslužitelje. Zatim se *keystroke logger* trojanskog konja potajno učitao na računala posjetitelja koji su surfali kompromitiranom Web lokacijom pomoću Internet Explorera. Download.ject je primjer pokretanja po preuzimanju.

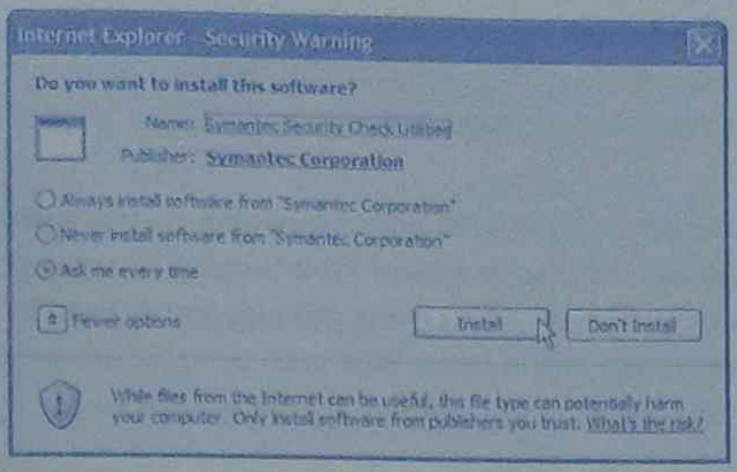
Druga taktika je korištenje pretraživača kao mehanizma za učitavanje zlonamjernog koda. Napadači mogu zavarati korisnika da preuzme softver (pomoću društvenog inženjeringa) ili prisiliti pretraživač da preuzme softver bez znanja korisnika, koristeći niske postavke zaštite. *Spyware* i *adware* često se oslanjaju na Web pretraživač da bi dobili ulaz na računalo korisnika.

Rad s ActiveXom

Jedan od razloga popularnosti Web pretraživača kao mehanizma transporta *spywarea* i *adwarea* je ActiveX. ActiveX je Microsoftova tehnologija koja Web stranice čini interaktivnijima – na primjer, kroz animacije ili kroz mogućnosti otvaranja drugih aplikacija u pretraživaču (kao što su Microsoft Word ili Adobe). Osim oživljavanja Web stranica, ActiveX tehnologija može izvršavati programe, koji se nazivaju ActiveX kontrole, na računalu preko Internet Explorera. ActiveX kontrole provode interakciju s operativnim sustavom kao bilo koji drugi izvršivi softver. Neke ActiveX kontrole su bezazlene i poboljšavaju iskustvo pretraživanja, ali pisci *malwarea* mogu ih također kreirati za instaliranje nepoželjnih programa na vaše računalo.

ActiveX provjerava digitalni potpis pridružen s komadom softvera koji će se preuzeti. Digitalni potpis potvrđuje vjerodostojnost kreatora softvera. Iako digitalni potpis ne jamči da je odnosni program siguran, on može pomoći u uočavanju programa koji se pokušavaju prerušiti kao druga vrsta softvera. Preporučuje se da ne prihvaćate softver s nevažećim digitalnim potpisom.

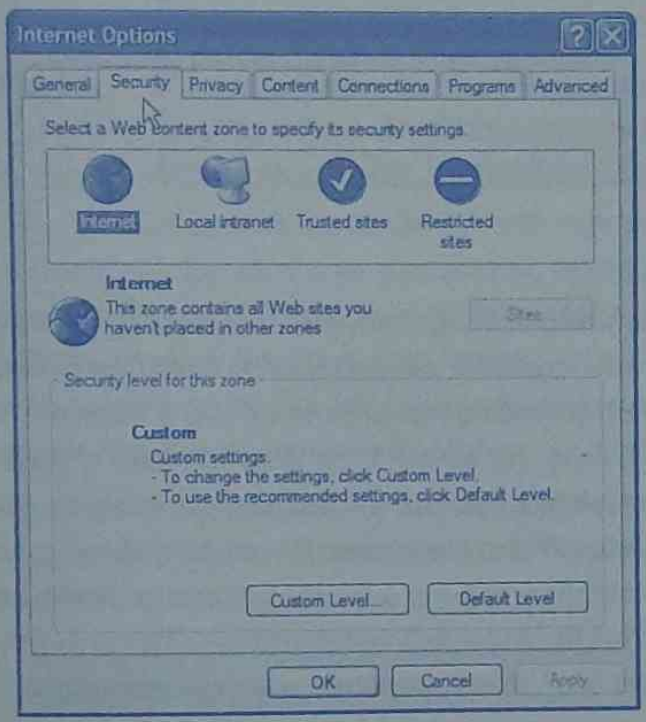
Postavke IE pretraživača možete podesiti tako da će on otvarati jedan prozorčić kako bi vas upozorio kada se neka ActiveX kontrola želi učitati na vaše računalo i omogućuje vam da odaberete hoćete li preuzetu kontrolu instalirati ili ne (pogledajte sliku 7.8).



Slika 7.8 Sigurnosno upozorenje Internet Explorera

Da biste provjerili postavku otvorite IE, odaberite Tools, a zatim Internet Options. To otvara prozor Internet Options.

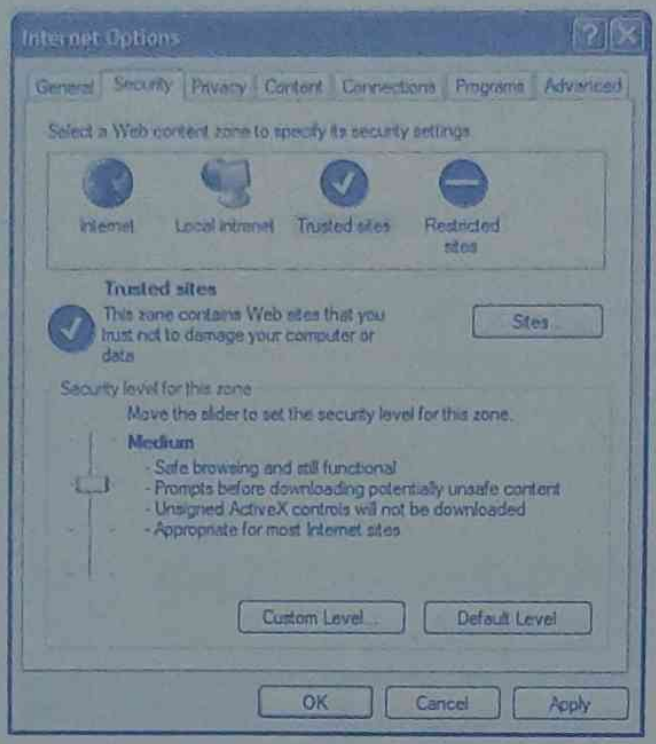
Kliknite jahač Security, kao što je prikazano na slici 7.9. Vidite četiri Web zone za koje možete podesiti postavke sigurnosti: Internet, Local intranet, Trusted sites i Restricted sites. Svaka zona ima vlastite postavke sigurnosti koje primjenjuje na svaku Web lokaciju koju dodajete zonama. One Web lokacije koje se ne nalaze na popisu u nekoj zoni imaju sigurnosne postavke zone Internet. (S postavkom Local intranet ne trebate ništa raditi jer je ona za Windows PC-e koji su dio korporativne mreže.)



Slika 7.9 Dijaloški okvir Internet Options otvoren na kartici Security

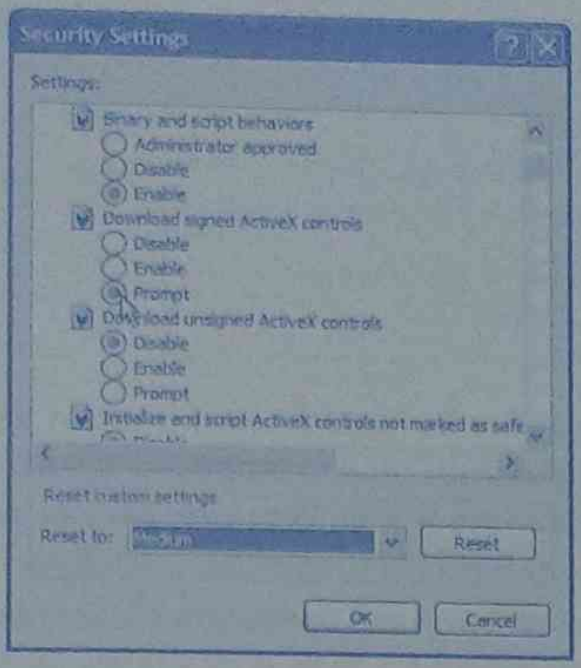
Da biste zonama Trusted Sites i Restricted sites dodali Web lokacije kliknite zonu koju želite podesiti pa kliknite gumb Sites... U dijaloškom okviru koji se otvorio jednostavno upišite Web adresu svake lokacije koju želite uključiti u odnosnu zonu.

Za svaku zonu možete promijeniti postavke sigurnosti da biste podesili upute za sigurnost i konfiguracije dodijeljene svakoj Web lokaciji koju ste dodali u zonu. Da biste promijenili postavke za svaku zonu, kliknite ikonu zone koju želite podesiti. Trebali biste vidjeti kliznu traku koja vam omogućuje promjenu postavki i koja je u rasponu od Low do High (pogledajte sliku 7.10).



Slika 7.10 Kartica Exceptions Windows Firewalla

Možete se poigrati i s pojedinačnim sigurnosnim značajkama klikom gumba Custom Level... To će otvoriti dijaloški okvir Security Settings prikazan na slici 7.11. Ovdje možete postaviti pojedinačna pravila za rad s ActiveX kontrolama i drugim funkcijama pretraživača. Na primjer, za Web lokacije u zoni Trusted, možete odabrati opciju Enable for the Download signed ActiveX controls. To znači da će se potpisane ActiveX kontrole preuzimati bez obavijesti. Za lokacije u zoni Internet možete odabrati Prompt kako bi vas računalo pitalo za dozvolu prije nego što počne preuzimati potpisane ActiveX kontrole. Za zonu Restricted možete odabrati Disable pa se ActiveX kontrole neće preuzimati.

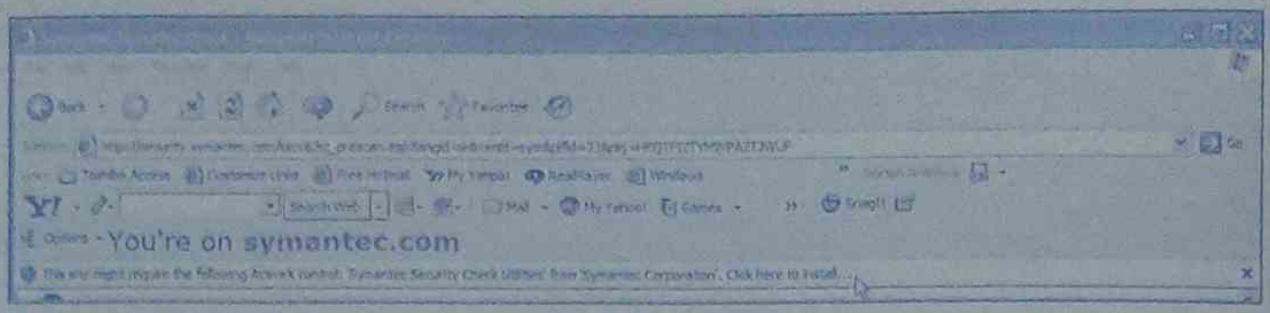


Slika 7.11 Prilagodba sigurnosnih postavki

Imajte na umu da podešavanje pojedinačnih postavki u prozoru Security Settings može utjecati za vaš doživljaj surfanja. Možete i odabrati jednu od opcija (High, Medium, Medium-Low ili Low) u području Reset custom settings ako se ne želite baviti s pojedinačnim postavkama. Ako ste to ipak učinili i sada ste potpuno zbunjeni, možete kliknuti gumb "Reset" kao što je prikazano na slici 7.11. To će postavke koje ste promijenili vratiti na osnovne Microsoftove postavke.

Zapamtite da tako dugo dok je postavka IE Security postavljena na Medium dobivat ćete poruku upozorenja; svaka druga niža postavka dopušta preuzimanje ActiveX kontrola bez obavijesti. Preporučljivo je da odaberete postavku Medium barem za zonu Trusted. Za zonu Internet ja bih najprije odabrao postavku High pa provjerio kvari li ona doživljaj surfanja. Zapamtite, lokacije kojima vjerujete možete uvijek postaviti u zonu Trusted s nižom postavkom. Međutim, ja ne bih išao niže od Medium za zonu Internet. Očigledno je da biste za lokacije u zoni Restricted trebali odabrati postavku High (ili jednostavno nemojte posjećivati lokacije koje biste postavili u zonu Restricted).

Windows XP SP2 dodaje alatnu traku (pod nazivom Information Bar) u Internet Explorer koja se pojavljuje kada se treba preuzeti neka potpisana ActiveX kontrola (pogledajte sliku 7.12). Information Bar se pojavljuje ispod drugih alatnih traka koje ste dodali u Internet Explorer. Kada kliknete Information Bar ona vam daje opciju da preuzmete ActiveX kontrolu ili dobijete više informacija o potencijalnim rizicima koje prihvaćate njezinim preuzimanjem.



Slika 7.12 Information Bar

Ako prihvatite preuzimanje, pojavit će se dijaloški okvir u kojem trebate potvrditi da želite instalirati softver. Ako je softver uredno potpisan, dijaloški okvir prikazuje naziv softvera i njegovog izdavača te daje Web veze kako bi vam pružio više informacija o softveru i njegovom izdavaču (pogledajte sliku 7.8).

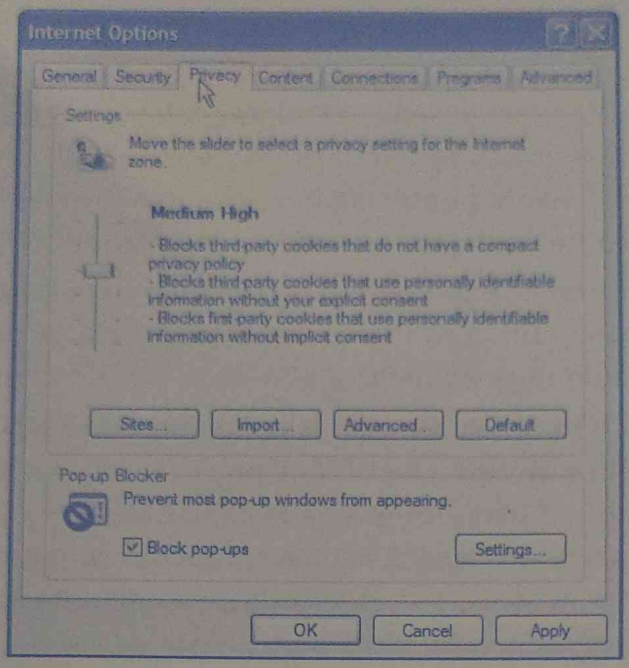
No, čak i ako se pojavi dijaloški okvir koji vas upozorava o nepotpisanoj ActiveX kontroli, klik gumba No neće uvijek pomoći. Neki pisci *malwarea* manipuliraju tim dijaloškim okvirom pa će se klikom gumba No ili nekog drugog gumba softver nastaviti preuzimati. Napadači mogu probati i modificirati tu poruku tako da ona izgleda kao poruka iz Windowsa ili kao da je generirana na Web lokaciji na kojoj se nalazite. Te su poruke alarmantne i uglavnom traže da odmah poduzmete neke akcije, poput klika gumba Yes za provođenje skeniranja ili preuzimanje programa za popravak "problema". Takve biste poruke trebali ignorirati.

Da biste zatvorili dijaloške i druge okvire bez klika gumba No ili Cancel ili X u gornjem desnom kutu možete pritisnuti Alt-F4. To će sigurno zatvoriti prozore unutar pretraživača bez omogućavanja preuzimanja bilo kakvog sadržaja.

Konfiguracija privatnosti

Prozor Internet Options ima pored kartice Security i druge opcije koje mijenjaju postavke Internet Explorera, uključujući General (gdje možete postaviti svoju polaznu stranicu, pohraniti privremene Internet datoteke i konfigurirati bilježenje stranica koje ste posjetili) i Privacy. Ovaj odjeljak detaljno opisuje postavke Privacy.

Postavke Privacy omogućuju vam da određujete kako će kolačići biti pohranjeni na vaše računalo (pogledajte sliku 7.13). Kolačić je mala datoteka koju Web lokacija pohranjuje na tvrdi disk vašeg računala da bi se prilagodila vašem načinu pretraživanja. Na primjer, kolačići pomažu lokacijama za e-trgovinu da zapamte interese korisnika. Kolačiće bi trebala pokrivati politika za privatnost Web lokacije. Politika za privatnost ističe način na koji Web lokacija sakuplja i dijeli informacije o svojim korisnicima. Općenito, kolačići su relativno bezopasni.



Slika 7.13 Podešavanje postavki kolačića u IE-u

Međutim, neki kolačići prate vaše surfanje Webom da vide koje druge lokacije posjećujete, ponekad s osobno prepoznatljivim informacijama, kao što su vaše ime i adresa. Te se informacije koriste za "istraživanje tržišta" koje pomaže u pružanju usmjerenijeg oglašavanja. Drugi se kolačići učitavaju na vaš tvrdi disk i nisu pokriveni politikom za privatnost.

Postavka Privacy sadrži kliznu traku koja konfigurira način na koji vaš pretraživač radi s kolačićima. Postavke su u rasponu od prihvaćanja do blokiranja svih kolačića. Pomicanjem klizača na traci prema gore, moći ćete vidjeti kako svaka postavka rješava pitanje kolačića koje postavlja neka Web lokacija koju posjećujete ili pitanje kolačića treće strane. Microsoft definira kolačiće treće strane kao one koji ne potječu iz iste domene kao i Web lokacija koju posjećujte. Kolačići treće strane su najvjerojatnije kolačići za praćenje. Moj je savjet za koristiti postavku High ili Medium-High.

Možete kreirati i smjernice za specifične Web lokacije. Kliknite gumb Sites... da biste lokacije dodali na popis koji uvijek prihvaća ili uvijek blokira kolačiće. Postavke sa klizača možete i poništiti aktivirajući elemente pod jahačem Advanced...

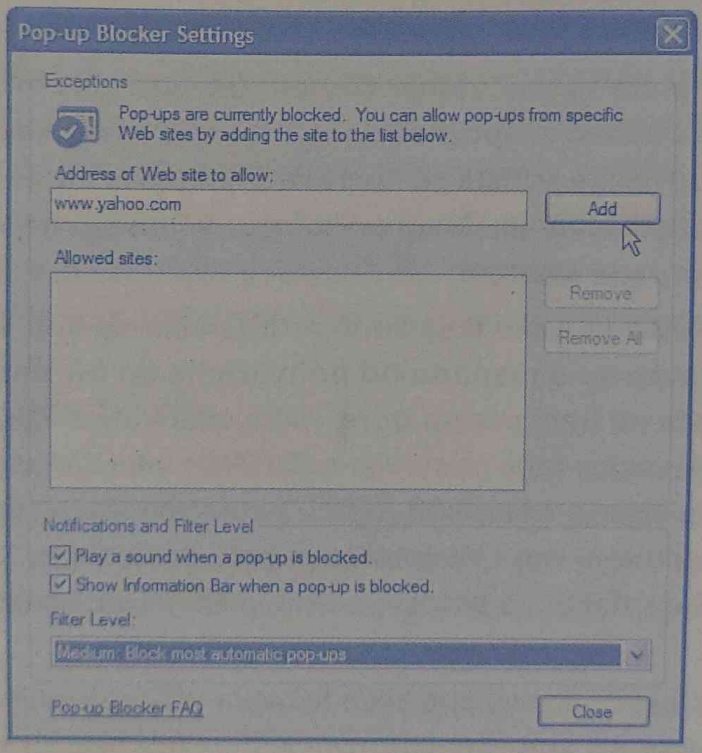
Zapamtite da se Web lokacije snažno oslanjaju na kolačiće da vam olakšaju pretraživanje. Ako blokirate sve kolačiće ili dobivate poruku u kojoj trebate prihvatiti kolačiće, trošit ćete dosta vremena na klikanje gumba Accept ili Deny tijekom posjeta Web stranicama.

Pop-Up Blocker

Mnoge Web lokacije tijekom vašeg posjeta generiraju iskočne oglase. Iskočni oglasi otvaraju nove prozore iznad stranice koju pregledavate. (Neki se prikazuju i ispod stranice; njih vidite nakon što zatvorite pretraživač. Ti se maštovito nazivaju "podskočni".) Ti su oglasi dosadni i potencijalno opasni jer *spyware* i *adware* koriste iskočne prozore kao način da vas navedu da instalirate njihove programe.

Windows SP2 koji izvodi Internet Explorer 6.0 omogućuje vam da preskočite te oglase pomoću opcije Pop-Up Blocker. Prema osnovnoj postavci ona je omogućena, ali je možete prilagoditi ili je isključiti.

Da biste uključili (ili isključili) Pop-Up Blocker, kliknite jahač Privacy u prozoru Internet Options. Vidjet ćete potvrdni okvir Block pop-ups na dnu dijaloškog okvira (pogledajte sliku 7.13). Za konfiguriranje kliknite Settings... Dijaloški okvir Pop-up Blocker Settings, prikazan na slici 7.14, omogućuje vam da izuzmete neke lokacije od funkcije blokiranja. Možete također odabrati način na koji ćete biti obaviješteni da je neka iskočna poruka blokirana.



Slika 7.14 Dijaloški okvir Pop-up Blocker Settings

Potom možete postavite razinu filtra na Low, Medium ili High. Low dopušta iskočne oglase sa sigurnih lokacija (odnosno s lokacija koje koriste HTTPS, kao što je Web lokacija vaše banke). Medium blokira većinu iskočnih oglasa, osim

onih koji dolaze s Web lokacija na popisu zone Trusted. Postavka High trebala bi blokirati sve iskočne oglase. Ja preporučujem postavku Medium ili High.

Možete i s Interneta preuzeti besplatne alate koji blokiraju iskočne oglase. Na primjer, Yahoo! i Google nude alatne trake za pretraživače koje mogu blokirati iskočne oglase. Posjetite adresu http://toolbar.yahoo.com ili http://toolbar.google.com. Alatne trake dostupne su i za druge pretraživače.

7.4 Alternativni pretraživači

Najbolji način da spriječite najčešće napade je da se klonite najpopularnijih meta. Kao što je već spomenuto, svaki softver ima mane i može se napasti, ali Microsoftov pretraživač Internet Explorer je nedvojben izbor napadača. Alternativni Web pretraživači kao što su Firefox i Opera su na dalekom drugom mjestu u utrci protiv Microsofta. Zato je velika prednost tih pretraživača ta što privlače manje pažnje kriminalaca s Interneta. Oni sadrže osnovne elemente kao što je blokiranje iskočnih oglasa i imaju čak i neke bolje značajke od Internet Explorera, poput tabelarnog pretraživanja, koje vam dopušta da u pretraživaču otvorite nekoliko prozora.

Osim slabije prodornosti na tržištu, drugi razlog veće sigurnosti tih pretraživača je da oni ne koriste ActiveX. Umjesto toga, oni koriste tehnologiju koja se naziva Java apleti. Poput ActiveXa, Java apleti mogu poboljšati doživljaj surfanja i pomoći kod preuzimanja softvera. Za razliku od ActiveXa, Java apleti nisu integrirani u operativni sustav računala što *malwareu* otežava dobivanje uporišta. Java apleti se izvode unutar nečega što se naziva sanduk za pijesak *(sandbox)*. Sanduk za pijesak izolira applet i daju mu pristup samo ograničenim resursima računala. Moguće je iskorištavanje i zlorabljenje Java apleta, ali općenito oni pružaju veću razinu sigurnosti.

Uz prije navedeno, ovi pretraživači nisu magična zaštita od napadača. Ako se odlučite za korištenje alternativnog pretraživača, sigurnosna mantra glasi "redovito ažurirajte svoj softver". Na primjer, najnovija verzija Firefoxa (trenutno je to verzija 1.0.7) adresira dvije kritične sigurnosne ranjivosti. Sami se morate brinuti da vam je softver ažuran i otkrivati zakrpe za najnovije otkrivene ranjivosti – automatski sustav ažuriranja, Windows Update, ne radi kod ne-Microsoft proizvoda.

Ironično, kako ove alternative postaju sve popularnije (mnogo je milijuna korisnika već preuzelo pretraživač Firefox), one će prirodno početi privlačiti više pažnje kriminalaca. Otkrivat će se više ranjivosti, pretraživači će se više zlorabiti te će završiti tako da će se njihova prednost u sigurnosti istopiti.

Druga loša strana je ta što su mnoge Web lokacije optimizirane za Internet Explorer, što znači da će alternativni pretraživač imati problema pri potpunoj inerpretaciji (renderiranje) Web stranice i svih njezinih funkcija. Na primjer, nisam mogao koristiti Firefox da bih naručio knjigu s Amazona; morao sam se prebaciti na IE da bih obavio transakciju. No, međutim, ne postoji pravilo koje kaže da se ne smije koristiti nekoliko pretraživača na jednom računalu. Mnogi ljudi koriste alternativni pretraživač za općenito surfanje po Webu i koristi IE samo kada je to neophodno.

Sljedeći odjeljci predstavljaju vam Firefox i Operu, dva najpopularnija alternativna pretraživača.

Firefox (www.mozilla.org)

Najpopularniji alternativni pretraživač je Firefox, dostupan za besplatno preuzimanje. Firefox se temelji na softveru otvorenog izvora; to znači da svatko tko želi, može dobiti kopiju izvornog koda. Izvorni kod je temeljni skup softverskih uputa koji upućuje aplikaciju ili program kako da radi. Korisnici su dobrodošli da kopaju po izvornom kodu kako bi pronašli bugove, predlagali poboljšanja i dodavali nove značajke i funkcije koje potom postaju dostupne preostalom dijelu korisničke zajednice. Većina softvera otvorenog izvornog koda je besplatna i održavaju ga dobrovoljci.

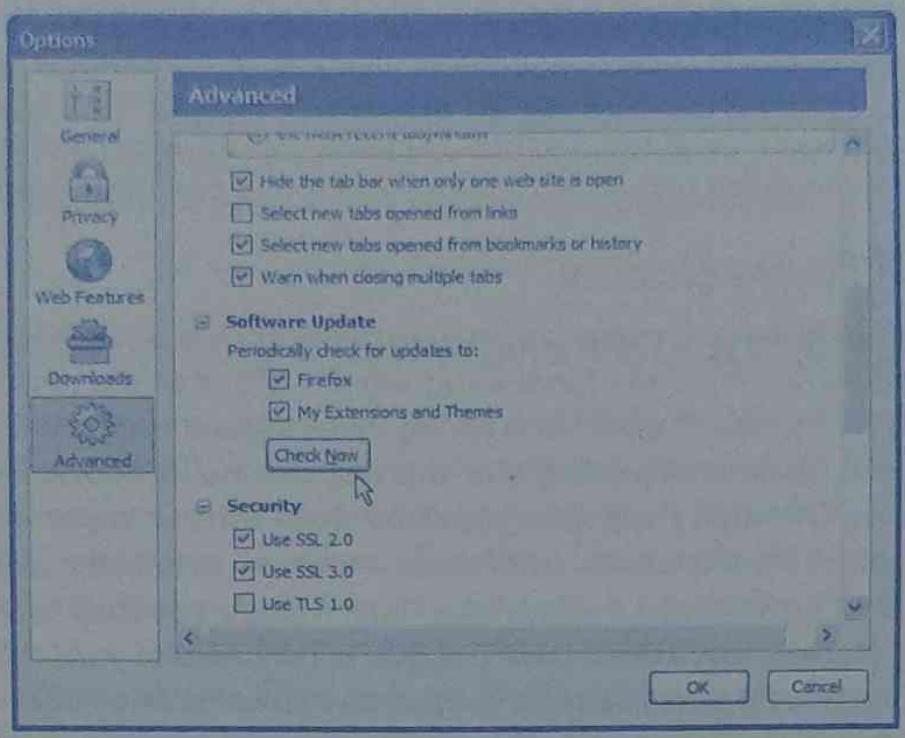
Suprotnost softveru otvorenog izvora je vlasnički softver. Izvorni kod vlasničkog softvera ljubomorno se čuva u kompaniji koja ga posjeduje. Nove značajke, funkcije i ispravke bugova kreira i objavljuje tvrtka vlasnik, prema vlastitom rasporedu.

Jedna od dobrih strana softvera otvorenog izvora je ta da na njemu odjednom radi mnogo različitih ljudi pa on dobiva zanimljive i zabavne dodatke. Te dodatke možete vidjeti (Mozilla ih naziva proširenjima) na adresi https://addons.mozilla.org/.

Kao što je već napomenuto, Firefox nije bez pogrešaka. On je i dalje podložan ranjivosti i potencijalnom zlorabljenju, i toga morate biti svjesni. Da biste vidjeli trenutni popis pukotina u pretraživaču posjetite Web stranicu www.mozilla.org/projects/security/known-vulnerabilities.html. Na njoj se nalazi popis pukotina koje su riješene s novim izdanjima softvera Firefox. Na stranici se nalaze i ocjene opasnosti za svaku pukotinu.

Da biste pronašli najnoviju verziju Firefoxa, uključujući i sigurnosne ispravke otiđite na www.mozilla.org/security/. Ako već koristite Firefox pa želite potražiti najnoviju nadogradnju, odaberite Tools pa Options, što otvara dijaloški okvir. U njemu kliknite Advanced. Otvorit će se dijaloški okvir prikazan na slici 7.15.

Pomaknite se prema dolje po ekranu dok ne dođete do retka Software Update. Ako potvrdite okvire Periodically check for updates to: Firefox će provjeravati Firefox Web lokaciju svaki dan da vidi ima li novih verzija softvera. Zapamtite da Firefox automatski ne instalira te nove verzije – on će vas pitati prije nego što počne instalirati bilo koji softver. Kada kliknete Check Now, Firefox automatski provjerava postoje li nove verzije softvera.



Slika 7.15 Provjera novih verzija softvera Firefox

Opera (www.opera.com)

Opera je dostupna u dvije verzije: jedna je besplatna a druga košta 39 američkih dolara. Besplatna verzija generira oglašavanje. Kada instalirate besplatnu verziju Opere, možete birati između dobivanja ciljanih oglasa s Googlea ili generičkih oglasa. Ako odaberete ciljane oglase s Googlea IP adresa vašeg računala i URL-ovi koje posjećujete slat će se na Google kao pomoć za generiranje oglasa koji odgovaraju vašim preferencama pretraživanja. Google također nastoji odrediti vašu geografsku lokaciju na temelju IP adrese da bi pomogao u ciljanom oglašavanju. Opera tvrdi da on ne sakuplja osobne informacije o vama. Detalje o tome naći ćete na adresi www.opera.com/adsupport/ and at www.opera.com/privacy.

Ja sam isprobao verziju s generičkim oglasima. Pretraživač ostavlja malu površinu u gornjem desnom kutu stranice za banner oglase; to nije napadno i zasigurno se može tolerirati. Ako vam se Opera zaista sviđa, ali ne možete podnijeti oglašavanje, kopiju možete licencirati za 39 američkih dolara, pa će oglasi nestati.

7.5 Provjere sigurnosti

Jedna je stvar postaviti vatrozid i namjestiti kontrole u Internet Exploreru, ali još je bolje provjeravati svoj rad. Internet je prepun izvora za provjeravanje sigurnosnog statusa vašeg računala. Tri ovdje opisana definitivno vrijedi istražiti.

ShieldsUP! (www.grc.com)

ShieldsUP! je besplatna usluga za provjeru sigurnosnih postavki osobnih vatrozidova, uključujući Windows Firewall ugrađen u SP2. Kao što smo spomenuli u 3. poglavlju, ShieldsUP! godinama vodi guru za sigurnost Steve Gibson. Lokacija nudi nekoliko testova, uključujući dva koja odgovaraju Windows Firewallu. Prvi, pod nazivom Common Ports, provjerava 26 često korištenih portova koji mogu biti otvoreni (i tako pristupačni i zločestim dečkima). Drugi test, pod nazivom Service Ports, provjerava 1.056 portova. To je mnogo opsežniji test i dulje traje. U svakom slučaju, rezultati su jasni i lako ih je razumjeti te vam mogu pružiti sliku o tome obavlja li vaš vatrozid svoj posao. Lokacija ima i veze do detaljnih informacija o osobnim vatrozidovima i sigurnosti računala.

Za pokretanje testova, otiđite na www.grc.com i pomaknite prikaz nadolje do veze ShieldsUP!. Korištenjem ove usluge dajete službenu dozvolu da pomoćni program ShieldsUP! skenira vaše računalo. ShieldsUP! vam daje IP adresu računala koje se koristi za skeniranje vašeg stroja, pa ako vas zanima, možete nakon skeniranja pregledati dnevnike svojeg vatrozida da vidite kako je skeniranje izgledalo iz perspektive vatrozida.

PivX PreView (www.pivx.com/preview)

PreView je besplatan sigurnosni alat iz tvrtke pod nazivom PivX. Alat ocjenjuje sigurnost vašeg računala na temelju četiri kategorije: Threat Center (centar za prijetnje), Security Software (sigurnosni softver), Patches/HotFixes (zakrpe/ispravke) i Firewall Protection (zaštita vatrozida). PreView analizira vaše računalo i

proračunava ocjenu sigurnosti koristeći ove četiri kategorije. To je jednostavan način da saznate koliko je vaše računalo ranjivo na napade. Međutim, velik dio u ocjeni temelji se na tome jeste li naručili neki PivX proizvod, pa uzmite ocjenu s malom zadrškom.

Symantec Security Check (www.symantec.com/securitycheck/)

Symantec Security Check skenira vaše računalo za razne potencijalne ranjivosti, uključujući portove koji mogu odgovarati na nepoželjne zahtjeve, prisutnost trojanskih konja i izvodi li se na računalu antivirusni softver. Rezultati testa su razumljivi, a detaljni su rezultati dostupni za Hacker Test (koji prikazuje portove koji odgovaraju ili ne odgovaraju zahtjevima za uspostavljanje veza). Ova provjera zahtijeva preuzimanje ActiveXa da bi mogla funkcionirati.

7.6 Internet Explorer 7.0 i Windows Vista (Longhorn)

Microsoft planira značajne nadogradnje za Internet Explorer i Windows operativni sustav. Internet Explorer 7.0 će vjerojatno biti dostupan krajem 2005. godine. Iako su za vrijeme dok sam pisao ovo poglavlje detalji bili šturi, Microsoft je obećao da će IE 7.0 uključivati brojne pojačane sigurnosne i nove alate da bi se poboljšalo iskustvo pretraživanja. Mnogi su promatrači očekivali da će Microsoft zadržati objavljivanje nove verzije IE-a dok tvrtka ne objavi novi operativni sustav. Međutim, Microsoft je razglasio datum izlaska nakon što se je uvidio nevjerojatan porast popularnosti Firefoxa i drugih alternativnih pretraživača. (No, bez obzira na to, Internet Explorer i dalje zauzima otprilike 90% tržišta pretraživača pa Firefox ima pred sobom još dugačak put do značajne popularnosti.)

Novi operativni sustav pod *radnim* nazivom Longhorn-Vista, očekuje se pri kraju 2006. godine. Ponovno, detalji su tajni, ali je Microsoft obećao nova sigurnosna poboljšanja kao i bolju grafiku i novi sustav za pohranjivanje datoteka te sposobnost da se Internet Explorer izvodi u ograđenom području što će *malwareu* otežati da koristi pretraživač kao ulaznu točku na vaše računalo.

7.7 Popis za provjeru

Upotrijebite ovaj popis za provjeru kao brzi referentni vodič kroz gradivo izneseno u ovom poglavlju.

Učinite

- Uključite opciju Automatic Updates da bi se osiguralo izvođenje najnovijih ispravki i sigurnosnih zakrpa Microsoftovog softvera.
- Iskoristite sigurnosne sposobnosti Windows Security Centera, uključujući vatrozid i antivirusni nadzor.
- Upotrijebite Windows Firewall ako nemate vatrozid nezavisnog proizvođača.
- Razmotrite korištenje alternativnog Web pretraživača za *surfanje* Internetom.
- Poduzmite korake koji osiguravaju da će vas Internet Explorer pitati prije nego što instalira ActiveX kontrole.

Nemojte učiniti

- Nemojte zaboraviti ažurirati Windows i Internet Explorer.
- Nemojte prihvatiti nepotpisane ActiveX kontrole.
- Nemojte zaboraviti ažurirati alternativne pretraživače s najnovijim softverskim ispravkama.
- Nemojte izvoditi istodobno dva ili više vatrozidova na istom stroju.

7.8 Korisni izvori

Ovaj odjeljak daje popis dodatnih izvora koji će vam pomoći da saznate više.

Microsoft ima brojne sigurnosne informacije za korisnike i dobro je mjesto za početak učenja o nekim osnovama o sigurnosti. Pođite na www.microsoft.com/athome/security da biste saznali više o osiguravanju Windowsa i Microsoft aplikacija.

CastleCops je korisnički forum za razne teme o računalima, uključujući sigurnost. Forumu se možete pridružiti da biste postavljali pitanja, čitali poruke i dobili korisne informacije o gotovo svemu pod svodom nebeskim što se odnosi na

računala. Posebno, ako odsurfate do http://castlecops.com/forums možete se pomicati po popisu da biste pronašli forume o pretraživačima (i njihovoj sigurnosti) i operativnim sustavima (uključujući Windows i sigurnost Windowsa).

Organizacija za istraživanje sigurnosti, Secunia, prati zakrpane i nezakrpane pukotine u Windowsima i nekoliko popularnih pretraživača, uključujući Internet Explorer i Firefox. Tekst je tehnički, ali lokacija je odlično ispitno mjesto za provjeravanje najnovijih ranjivosti koje mogu utjecati i na vaše računalo. Posjetite www.secunia.com.

8. poglavlje

Sigurnost vaše obitelji na Internetu

Internet predstavlja priličan problem za savjesne roditelje. Bilo da nastojite isključiti loš materijal kao što je pornografija ili nasilje ili spriječiti grabežljivce djece koji se šuljaju sobama za čavrljanje, Internet otvara beskonačan broj avenija do Web lokacija i Web stanovnika koje ne želite u vlastitom domu. U drugu pak ruku, roditelji će se možda željeti zaštititi od posljedica postupaka svoje djece. Glazbena i filmska industrija u današnje vrijeme vrlo ozbiljno uzimaju kršenje autorskih prava, pa biste se mogli naći pod sudskim tužbama ili biti kažnjeni novčanim kaznama jer je vaše dijete preuzelo film *Star Wars: Episode III – Revenge of the Sith* ili glazbeni hit bez plaćanja vlasniku autorskih prava dijela koji mu pripada.

U korporativnom svijetu nekoliko tvrtki pretvorilo je filtriranje Weba u vrlo profitabilan posao. Njihovi proizvodi sadrže dugačke popise lokacija koje neke tvrtke ne žele da posjećuju njezini zaposlenici zbog odgovornosti (pornografija na radnom mjestu može predstavljati neprijateljsko okruženje i rezultirati sudskom tužbom) ili zbog produktivnosti (sportovi, kockanje i lokacije za e-trgovinu mogu odvlačiti zaposlenike od njihovog posla). Korporacije investiraju i u tehnologije da bi otkrile i blokirale programe za izravnu razmjenu datoteka koje omogućuju kršenje autorskih prava.

Slična tehnička rješenja dostupna su za kućnu upotrebu (iako ona nisu tako opsežna i nisu otporna na glupost), ali roditelji mogu iskoristi alate koji nisu tehnološke prirode i upotrijebiti zdrav razum i roditeljsku pažnju kad su kod kuće.

Ovo poglavlje iznosi rješenja za isključivanje nepoželjnih materijala s Weba. Govorit ćemo i o potencijalnim zakonskim i financijskim posljedicama razmjene datoteka i pregledati neke od problema sigurnosti koji su pridruženi softveru za izravnu razmjenu datoteka. Raspravljat ćemo i o pitanjima *online* sigurnosti kao što je zaštita vaše djece od *online* grabežljivaca. Neki od problema o kojima ćemo ovdje raspravljati imaju tehnička rješenja ili u najmanju ruku postoje alati koji će vam pomoći da te probleme riješite. No u većini slučajeva najbolja je obrana usađivanje dobrih navika za korištenje Interneta u znatiželjne glavice vaše djece. Zapamtite da je Internet kao i sve ostale zajednice – i on ima svoja sigurna područja i ona opasna, a staro pravilo da se ne razgovara sa strancima i dalje vrijedi.

8.1 Filtriranje nepoželjnog sadržaja

U doba kada sam ja bio dijete postojale su samo tri avenije do zabranjenog materijala: pronalaženje pikantnih dijelova u popularnim romanima koje su moji roditelji držali u kući, pregledavanje odbačenih časopisa s golim djevojkama i mukotrpno čekanje kod prijatelja koji su imali kabelsku televiziju do kasnih noćnih sati da počnu filmovi za one iznad 18 godina kako bismo vidjeli djelić golog ženskog tijela.

Ovih se dana situacija znatno promijenila. Internet je najveće svjetsko spremište prljavog sadržaja, koje je udaljeno samo nekoliko upita. To ne bi trebalo predstavljati iznenađenje. Pornografija je prodrijela u gotovo svaki masovni medij koji su ljudi otkrili, uključujući fotografije, tisak, film, kabelsku televiziju i kućni video. Jedini medij koji ne postiže velike prihode od pornografije je radio (iako se čini da Howard Stern i tu utire put). Ne znam kada je prva slika s obnaženim ljudskim tijelom prenesena s jednog na drugo računalo telefonskom linijom, ali se mogu kladiti da se to zbilo unutar prvog tjedna spajanja računala.

A pornografija je samo jedna od glava Hidre s pokvarenim sadržajem; postoji nasilje, kockanje, sobe za čavrljanje, rasističke lokacije itd. Složenost problema je u tome što Internetu nedostaju mnogi filtri koji postoje u drugim medijima. Na kiosku neće 11-godišnjem dječaku prodati *Playboy* (?) ali će mu Web pretraživač poslušno servirati tone lošeg sadržaja.

Roditeljima je pri ruci mnogo tehničkih i netehničkih opcija. Mi imamo nekoliko ideja za nadziranje *online* aktivnosti vaše djece i objašnjavamo kako koristiti filtre

tražilica i Web pretraživača. No, s obzirom na nevjerojatan broj opcija za isporuku sadržaja, najsigurnije rješenje (osim prekidanja veze s Internetom) će vjerojatno podrazumijevati softver za nadzor nekog nezavisnog proizvođača.

Ljudski nadzor

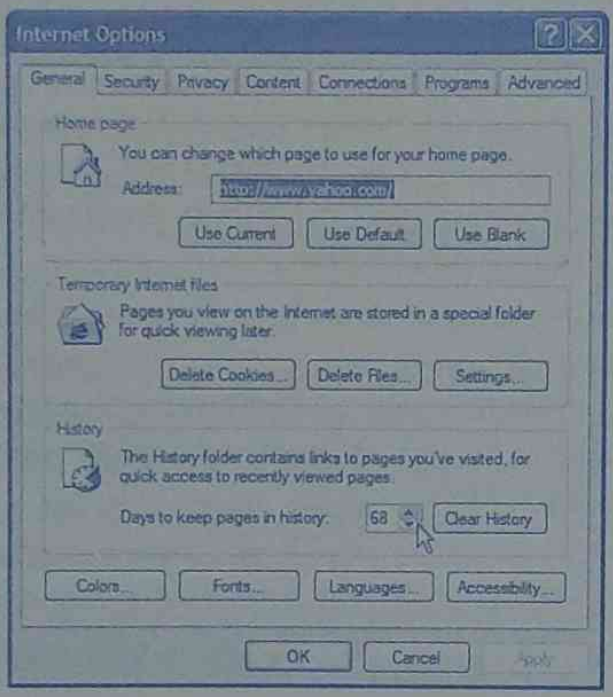
Najjednostavniji filtar je da svojoj djeci ne dopustite pristup Internetu u njihovim sobama. Ako odredite da je računalo u zajedničkom prostoru poput dnevnog boravka ono koje djeca smiju koristiti za *online* aktivnosti, moći ćete do neke mjere utjecati na njihovu *online* aktivnost. Saznanje da će svatko tko prolazi pokraj računala moći vidjeti što se nalazi na ekranu trebalo bi klincima onemogućiti pregledavanje lošeg sadržaja koji bi inače tražili. To može biti teško provedivo u kućanstvu u kojem nekoliko osoba treba istodoban pristup Internetu ili ako je instalirana bežična pristupna točka koja pokriva cijelu kuću. No dobro obiteljsko pravilo "Ako si na Internetu, onda budi u dnevnom boravku ili u kuhinji" ili neka varijanta ovoga trebala bi pomoći.

Uvijek možete pregledati što su vam djeca *online* radila provjeravanjem zapisa History u Web pretraživaču. Svaki Web pretraživač ima područje u kojem možete vidjeti svaku stranicu koju ste posjetili unutar određenog vremenskog razdoblja poput tjedna ili mjeseca. Možete kliknuti na lokaciju s popisa i posjetiti stvarne Web stranice, a neki vam pretraživači omogućuju pretraživanje zapisa History za specifične lokacije. Sama funkcija History korisna je za praćenje akcija koje želite ponovno posjetiti ali se ne možete sjetiti točne adrese. Ona je korisna i za nadziranje Internet aktivnosti vaše djece.

Da biste u Internet Exploreru pregledali History (slika 8.1) odaberite View, Explorer Bar, History. Unutar zapisa History možete kliknuti View da biste dobili različite opcije za pregledavanje zapisa: prema datumu, prema lokaciji, prema učestalosti posjeta ili prema redoslijedu posjeta.

Da biste postavili broj dana tijekom kojih će se pamtiti stranice, odaberite Tools, Internet Options. Pojavljuje se mali prozor koji duž vrha ima nekoliko jahača. Odaberite jahač General koji prikazuje okvir za konfiguriranje postavki opcije History (slika 8.2). Zapise lokacija možete spremati od 0 do 999 dana, ali bi nekoliko tjedana trebalo biti dovoljno.

Slika 8.1 Pregledavanje povijesti u Internet Exploreru



Slika 8.2 Postavljanje broja dana tijekom kojih će se pamtiti posjećene Web stranice

Ako koristite Firefox, povijest posjećenih stranica možete pregledati klikom View, Sidebar, History. Pojavit će se prozor duž lijeve strane pretraživača. Kao i u Internet Exploreru i ovdje možete upotrijebiti gumb View da biste pregledavali povijest prema datumu, lokaciji, najposjećenijoj lokaciji i posljednjoj posjećenoj lokaciji. Trajanje zapisa History možete odrediti odabirom Tools, Options. U prozoru Options kliknite ikonu Privacy. To otvara manji prozor koji sadrži polje za konfiguriranje opcije History.

Besplatna verzija pretraživača Opera ima vrlo jednostavan pristup zapisima posjećenih lokacija, i ikonu označenu s History u oknu na lijevoj strani pretraživača. Možete i odabrati Tools, History. Da biste provjerili koliko se dugo lokacije čuvaju odaberite Tools, Preferences. Kada se otvori prozor kliknite History na dnu popisa s lijeve strane prozora. Za razliku od IE-a i Firefoxa, Opera ne pohranjuje lokacije po datumu. Umjesto toga, možete odabrati broj lokacija koje će pohraniti, od 0 do 10.000; kada se dosegne maksimalan broj lokacija, stare se lokacije brišu kako se nove dodaju.

Možda ste primijetili da svaki pretraživač sadrži i gumb Clear History, kao što je prikazano na slici 8.2. Klikom ovog gumba brišu se trenutni zapisi History. Iako će vas to spriječiti od pregledavanja lokacija koje su vaša djeca posjećivala, to također može značiti da su možda posjećivala lokacije za koje ne žele da vi saznate. Zato, jedno od obiteljskih pravila koje postavite može biti da nitko ne smije koristiti gumb Clear History.

Nemojte se osjećati kao špijun pri nadziranju *online* aktivnosti; ne radite ništa loše. Zapravo, ako svojoj djeci kažete da provjeravate njihovu Internet aktivnost, to bi moglo pomoći da ona svladaju svoje nestašne porive.

Filtriranje tražilice

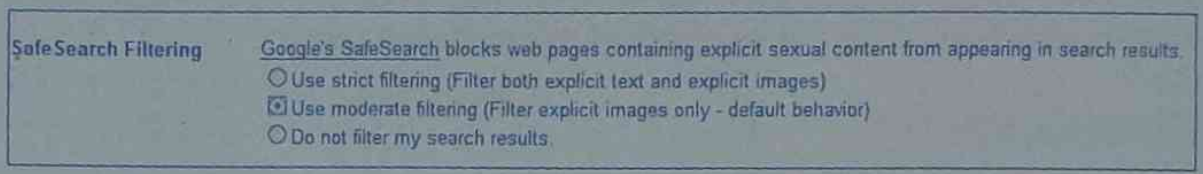
Popularne tražilice mogu se postaviti da filtriraju eksplicitni seksualni sadržaj iz pretraživanja po ključnoj riječi ili po slikama. Filtriranje tražilice ne zahtijeva dodatan softver i jednostavno se konfigurira. Međutim, te tražilice ne jamče da u svojim rezultatima pretraživanja neće dati i nepoželjni materijal. Jednako je tako jednostavno uključivati i isključivati filtriranje. Uz to, te postavke morate spremiti u svakoj tražilici i Web pretraživaču koji koristite. Na primjer, ako postavite Strict filtering za Google pomoću Internet Explorera, ta se postavka neće primjenjivati u Googleu ako koristite Firefox dok ga posebno ne konfigurirate. I konačno, pokušavanje konfiguriranja svake moguće dostupne tražilice na Internetu je beskorisno.

Pa postoji li uopće jedan razlog da se time gnjavite? Postoji. Konfiguriranje filtra na glavnim tražilicama osigurava dodatni sloj zaštite i prenosi svakome tko koristi Web ideju da je eksplicitan materijal nedopušten. Drugo, to može pomoći da

mlađu djecu (koja ne pokušavaju zaobići roditeljske zabrane) čuvate od slučajnog pronalaska zabranjenog sadržaja.

- Google filtriranje ima tri postavke: Strict filtering, koja uklanja eksplicitni seksualni sadržaj iz rezultata pretraživanja po slikama ili ključnim riječima; Moderate, koja filtrira samo eksplicitne slike (to je osnovna postavka); i No Filtering, koja otvara vrata svemu. Da biste odabrali postavku kliknite vezu Preferences na polaznoj stranici Googlea, kao što je prikazano na slici 8.3. To otvara stranicu koja vam omogućuje da podesite određene postavke, uključujući sekciju pod nazivom SafeSearch. Pomaknite se dolje do područja SafeSearch Filtering i odaberite jednu od postavki, kao što je prikazano na slici 8.4. Tada možete spremiti svoje preference, ali njih može promijeniti svatko tko koristi pretraživač.

Slika 8.3 Veza Preferences na polaznoj stranici Googlea



Slika 8.4 Googleovo područje SafeSearch

- Yahoo! nudi SafeSearch filtriranje s tri postavke: filtriranje eksplicitnog sadržaja s Weba, slika i pretraživanja videa; filtriranje pretraživanja slika i videa; i nikakvo filtriranje. Da biste odabrali postavku kliknite vezu Advanced na polaznoj stranici Yahoo!a. Otvorit će se stranica Advanced Web Search. Pomaknite se prema dolje do područja SafeSearch Filter gdje možete odabrati svoje postavke filtriranja. Zapamtite da se postavka primjenjuje samo na to pretraživanje. Da biste postavku primijenili na sva pretraživanja kliknite vezu "preferences". To će otvoriti prozor pod nazivom Search Preferences. Možete podesiti postavku za filtriranje pretraživanja te

je spremiti klikom gumba Save Preferences u gornjem desnom kutu. Problem s ovom postavkom je u tome što je lako može isključiti svatko tko koristi računalo. Yahoo! nudi i opciju za zaključavanje vaših preference pretraživanja, ali se morate registrirati kao Yahoo! korisnik. Kliknite vezu Log In, upišite u Yahoo! svoje korisničko ime i lozinku, odaberite svoju postavku i potvrdite okvir da zaključate SafeSearch u odabranom modu. Zatim možete kliknuti Save Preferences. No kako Yahoo! napominje na lokaciji, svatko tko se prijavi na računalo kao da ima 18 ili više godina može jednostavno zaobići Yahoo! postavke.

- MSN Search nudi tri razine filtriranja: Strict, koji filtrira seksualno eksplicitni tekst i slike; Moderate, koji filtrira eksplicitne slike i Off (isključeno filtriranje). Prijeđite na www.msn.com i kliknite gumb Search uz polje za pretraživanje. To otvara novi prozor. Da biste odabrali razinu filtriranja kliknite gumb Settings. Postavku možete spremiti, ali ne postoji način da nekog drugog, koji koristiti to računalo spriječite da je promijeni.

Filtriranje Internet Explorera

Upotrebom sposobnosti Internet Explorera možete dobiti strožu razinu filtriranja. Tako ćete izbjeći problem podešavanja postavki na velikom broju tražilica (iako ja preporučujem postavljanje filtra u svim glavnim tražilicama uz pretraživače). No, imajte na umu da je sustav filtriranja IE-a pomalo zbunjujući za postavljanje i održavanje te da sustav procjenjivanja ima pukotine.

IE ima filtriranje pretraživača pod nazivom Content Advisor. Međutim prema Web lokaciji za RSACi, ovaj sustav procjenjivanja je sada izvan funkcije i predan je Internet Content Rating Associationu (ICRA). Content Advisor može koristiti sustav procjenjivanja organizacije pod nazivom SafeSurf. Pogledat ćemo kako se postavlja Content Advisor da radi s ICRA-om.

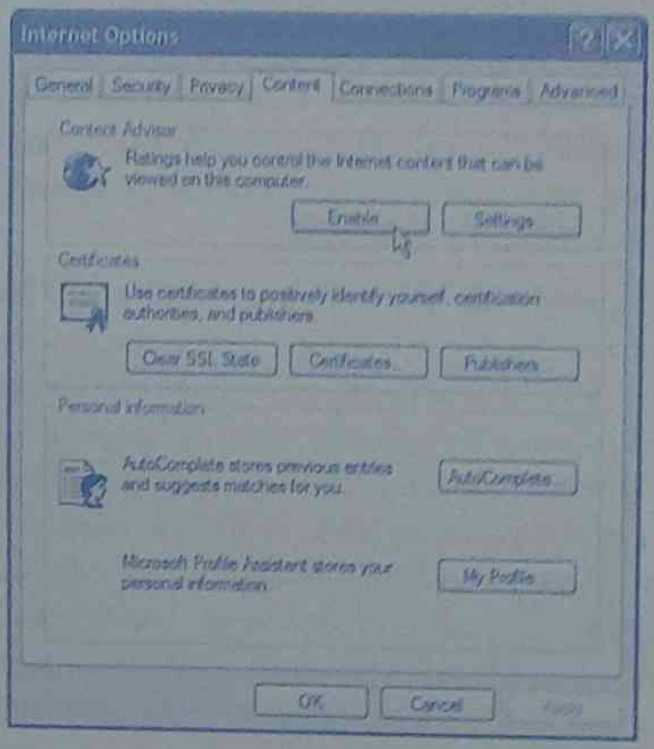
ICRA je razvila rječnik koji opisuje pet glavnih tema: Nudity and Sexual Content (golišavost i seksualni sadržaj), Violence (nasilje), Language (jezik), Chat Facilities (mehanizmi za čavrljanje) i temu iznenađenja koja obuhvaća kockanje i drogu. Operatori Web lokacije ispunjavaju upitnik koji ocjenjuje sadržaj lokacije koristeći 45 opisa pridruženih uz pet tema. Na primjer, ako Web lokacija ima sadržaj koji potpada pod temu Nudity and Sexual Content, ta lokacija može indicirati prisutnost muških ili ženskih genitalija i eksplicitne seksualne činove. Na temelju rezultata upitnika, ICRA generira komadić koda koji operator Web lokacije prilaže lokaciji. Internet Explorer provjerava postoji li taj kod pa potom dopušta ili zabranjuje pristup lokaciji na temelju postavki koje ste odabrali u Content Advisoru.

Zapamtite da ICRA ne istražuje škakljive lokacije koje će označiti; operateri Web lokacija dobrovoljno sudjeluju u njezinom programu i sami ispunjavaju upitnik. Očita pukotina u ovom sustavu je da ICRA ne može ništa učiniti s lokacijama koje nisu označene. Moja je pretpostavka da većina pornografskih, nasilnih i kockarskih lokacija nije označena. (Brza provjera pomoću ICRA-inog sustava testiranja pokazala je da Playboy.com ima oznaku ICRA ali Penthouse.com nema.) Uz to, malo je toga što se može napraviti da se operatera Web lokacije zaustavi od falsificiranja informacija u upitniku.

SafeSurf koristi sličan sustav ocjenjivanja da bi pokrio sličan skup tema uključujući heteroseksualne i homoseksualne teme, glorificiranje drogiranja i nasilje. Poput ICRA-e, SafeSurf je dobrovoljan sustav za vlasnike Web lokacija.

Da biste koristili sustav ocjenjivanja ICRA-e unutar Content Advisora, najprije morate preuzeti datoteku za ocjenjivanje (koja se skraćeno naziva .rat). Tu ćete datoteku preuzeti na adresi www.icra.org/faq/contentadvisor/setup/. Odaberite opciju Save na ekranu za preuzimanje datoteka. Zatim je spremite na svoje računalo (ako koristite Windows XP) u mapu C:\WINDOWS\System32. Ova Web lokacija je i dobar priručnik za podešavanje postavki Content Advisora nakon što ste dodali ICRA .rat datoteku.

Sada je vrijeme da postavimo Content Advisor u Internet Exploreru. Odaberite Tools, Internet Options. To otvara prozor Internet Options kao što je prikazano na slici 8.5. Kliknite jahač Content. Zatim kliknite Enable u sekciji Content Advisor.

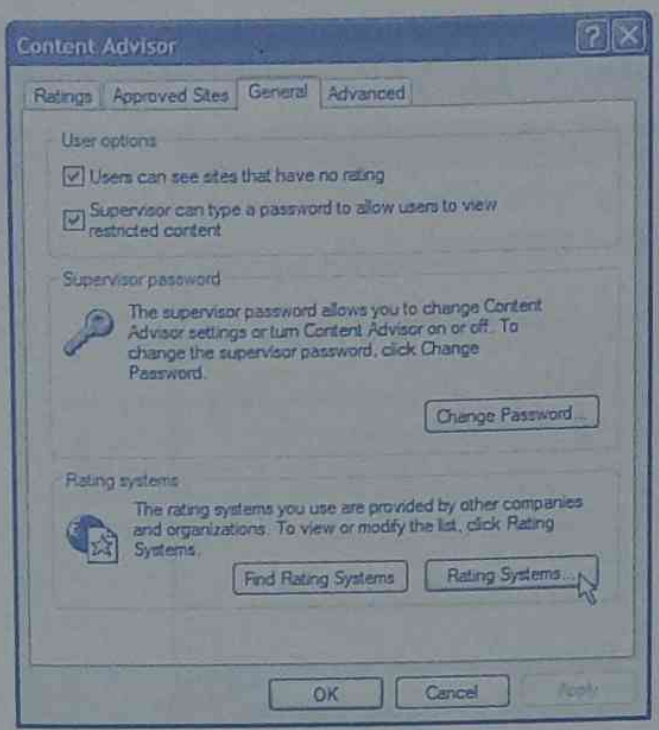


Slika 8.5 Kartica Content dijaloškog okvira Internet Options

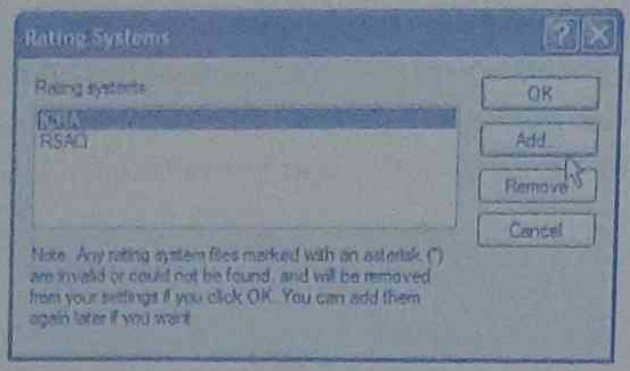
Kada postavite Content Advisor, on će tražiti da odaberete neku lozinku. Ta vas lozinka čini Supervisorom (nadzornikom). Kao Supervisor možete kontrolirati postavke Content Advisora i dopustiti ili zabraniti određene lokacije. Svakako odaberite lozinku koju nećete zaboraviti, ali i onu koju vaša djeca neće moći pogoditi.

> I Microsoft i ICRA strogo preporučuju da budete posebno pažljivi kod biranja lozinke, jer ako je zaboravite, nećete moći isključiti sustav filtriranja sadržaja, pa biste si mogli blokirati pristup lokacijama koje želite posjetiti. Ni Microsoft ni ICRA nemaju kopiju te lozinke, pa vam neće moći pomoći ako je izgubite.

Nakon što ste odabrali lozinku, trebate odabrati ICRA .rat datoteku. U dijaloškom okviru Internet Options (prikazanom na slici 8.5), kliknite gumb Settings. To otvara prozor pod nazivom Content Advisor, kao što je prikazano na slici 8.6. Kliknite jahač General, a zatim kliknite Rating Systems.... To otvara manji prozor s opcijama za dodavanje i uklanjanje sustava ocjenjivanja, kao što se vidi na slici 8.7. Sustav RSACi će vjerojatno biti na popisu. Trebate ga ukloniti, jer više ne radi. Trebate i dodati ICRA .rat datoteku koju ste preuzeli.



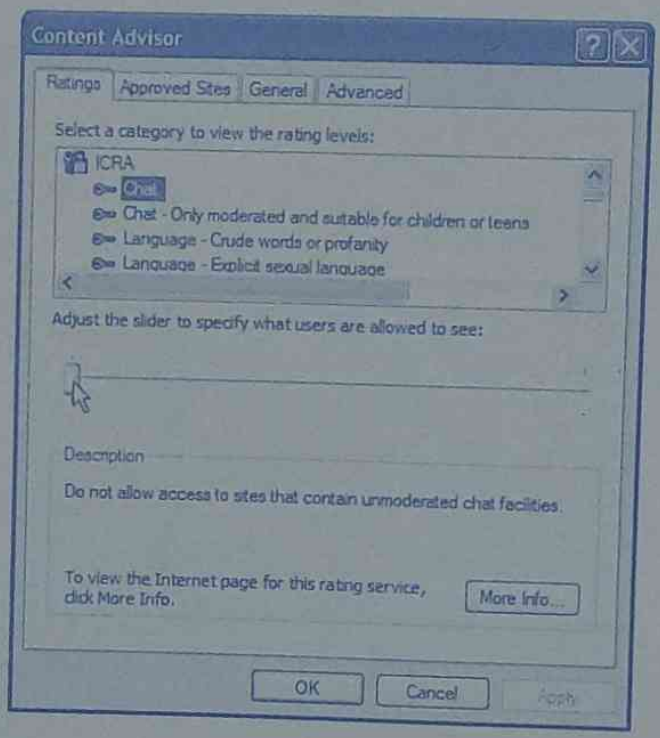
Slika 8.6 Kartica General dijaloškog okvira Content Advisor



Slika 8.7 Dijaloški okvir Rating Systems

Da biste dodali ICRA .rat datoteku kliknite gumb Add. To bi trebalo otvoriti datoteku system32, u koju ste spremili ICRA datoteku. Dvostruko kliknite ICRA datoteku. Ona bi se sada trebala nalaziti u okviru Rating Systems. Odaberite opciju ICRA i kliknite OK.

Sada nastavite s karticom Ratings u prozoru Content Advisor, kao što je prikazano na slici 8.8. Trebali biste na popisu vidjeti ICRA. Možete podesiti brojne kategorije uključujući Chat, Language, Nudity itd. Ako kliknete neku kategoriju pojavit će se klizna traka. Ona vam nudi dvije postavke: allow the category described (dopustiti opisanu kategoriju) ili deny the category described (zabraniti opisanu kategoriju). Osnovna postavka je u pravilu – zabraniti. Content Advisor ne podržava neke kategorije, a ICRA ocjenjivanje vas pita želite li klizač ostaviti na krajnjem desnom dijelu trake.



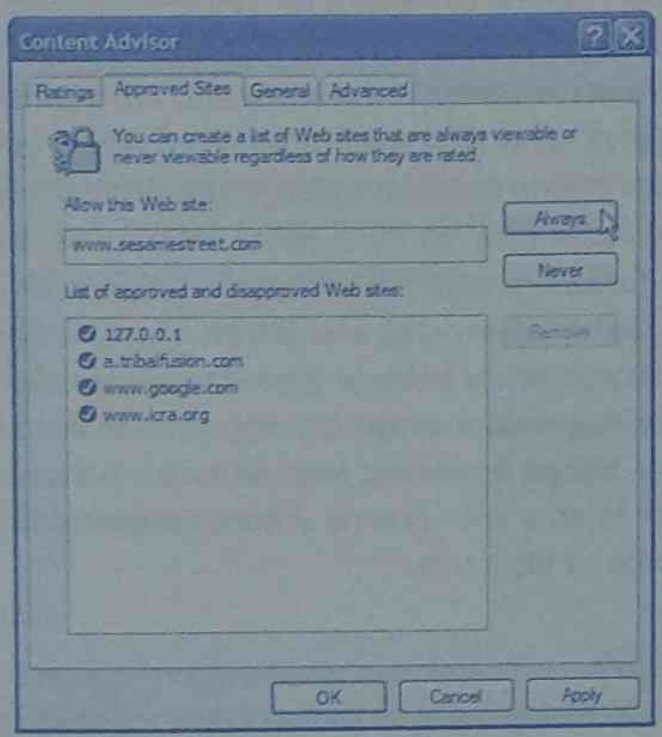
Slika 8.8 Kartica Ratings dijaloškog okvira Content Advisor

Nakon što podesite svaku postavku kliknite Apply. Tada možete prijeći na karticu General da biste postavili osnovne odrednice za korisnika (pogledajte sliku 8.6). Zapamtite da zbog toga što je ICRA dobrovoljni sustav ocjenjivanja, Web lokacije ne moraju u njemu sudjelovati, što znači da za te lokacije nema dostupnih ocjena. Content Advisor možete konfigurirati tako da omogući korisnicima pregledavanje neocijenjenih lokacija. Ili ga možete konfigurirati tako da Supervisor (a to ste vi) mora upisati lozinku da bi korisnici mogli vidjeti neocijenjene lokacije.

Testirao sam ovaj sustav tako da blokira sve Web lokacije koje nemaju ocjene. Neke od lokacija blokirane su samo zbog toga jer nemaju ocjenu, kao što su PBSKids.org, SesameStreet.com, ThomasTheTankEngine.com (da, ja imam djecu), StarWars.com, ESPN.com, eBay.com, CNN.com i Yahoo.com.

Kao što vidite, ako blokirate sve lokacije koje nisu ocijenjene blokirat ćete mnoge bezopasne lokacije kao i one s eksplicitnim sadržajem. Međutim, ako ne blokirate neocijenjene lokacije, kratki će test pokazati mnogo pornografskih lokacija, pa im Content Advisor dopušta da se probiju ako ste ga konfigurirali tako da ne blokira neocijenjene lokacije.

Što napraviti? Jedna je opcija unaprijed učitati sustav s dopuštenim lokacijama. To možete učiniti otvaranjem prozora Content Advisor, klikom opcije Settings, a zatim klikom jahača Approved Sites (pogledajte sliku 8.9). Zatim upišite vrstu URL-ova lokacija koje će uvijek biti dopuštene. (Možete upisati i lokacije koje će uvijek biti zabranjene.)



Slika 8.9 Kartica Approved Sites dijaloškog okvira Content Advisor

Isto tako, ako blokirate neocijenjene lokacije, Supervisor ima opciju premještanja blokiranih lokacija na popis Allowed uz naravno, korištenje lozinke Supervisora. Svaki put kada Content Advisor blokira neku Web stranicu Supervisor možete odabrati jednu od ove tri opcije: always allow the Web site to be viewed (uvijek dopusti pregledavanje Web lokacije), always allow the specific Web page to be viewed (uvijek dopusti pregledavanje određenih Web stranica) ili allow viewing only during that session (dopusti pregledavanje samo tijekom ove sesije). Morate upisati lozinku Supervisora da biste mogli odabrati jednu od ovih opcija.

Zato, ako koristite značajku Content Rating, morate provesti dosta vremena za postavljanje dopuštenih lokacija u ovu sekciju. Mogli biste i iznervirati članove svoje obitelji ako otkriju da su bezopasne lokacije blokirane, a vas nema u blizini da skinete blokadu. Ako vam to ne smeta, Content Advisor nudi vrlo jak mehanizam filtriranja za Internet Explorer. Međutim, ako niste spremni na premještanje dopuštenih lokacija i ne sviđa vam se ideja da maknete blokadu s neocijenjenih lokacija tada Content Advisor neće biti osobito efikasan pri izdvajanju nepoželjnog materijala.

Filtriranje alternativnih pretraživača

Koliko ja znam, popularni alternativni pretraživači kao što su Firefox i Opera (besplatna verzija), nemaju nikakve ugrađene mehanizme za filtriranje Web sadržaja. Zato, ako imate instalirane neke od ovih pretraživača na svojem računalu, vaša će djeca moći jednostavno zaobići Content Advisor. No, Firefox zajednica stalno gradi proširenja pretraživača. Dok sam pisao ovo poglavlje, nisam mogao locirati ni jedan projekt za filtriranje lošeg Web sadržaja, ali to bi se moglo promijeniti. Najbliža stvar koju sam mogao pronaći je proširenje pod nazivom Image-Show-Hide. Prema kratkom opisu, to vam proširenje omogućuje da prikažete ili sakrijete sve slike na Web stranicama. Ali radi se o jednom gumbu koji uključuje ili isključuje funkcioniranje proširenja, pa se ono lako zaobiđe. Uz to, proširenje zapravo ne filtrira loš sadržaj: ako ste ga uključili, ono skriva slike na svakoj Web stranici koju posjećujete, što je pomalo ekstremno. Ovo proširenje možete pronaći na adresi https://addons.mozilla.org/; kliknite vezu za Firefox extensions, a zatim vezu za Image Browsing, koja se nalazi u stupcu na lijevoj strani stranice. Možda ćete htjeti s vremena na vrijeme posjećivati Web stranicu da vidite postoji li proširenje za filtriranje.

Kontrole davatelja usluga

Mnogi davatelji usluga nude mehanizme za *online* zaštitu djece i pružaju sigurno surfanje Webom. Najbolji način da saznate što se nudi je da posjetite polaznu

stranicu svojeg davatelja usluge ili nazovete službu za korisnike. U međuvremenu, ovdje se nalazi popis kontrola za roditelje koje nude tri glavna davatelja usluga u SAD-u. Da biste imali pravo na te usluge morati biti njihov pretplatnik.

- AOL nudi nekoliko značajki kontrola za roditelje, uključujući AOL Guardian, koji roditeljima e-poštom šalje "karticu izvještaja", a u njoj su prikazane aktivnosti dopisivanja e-poštom, surfanja i dopisivanja u realnom vremenu *(instant messaging -IM)*. Druge značajke obuhvaćaju mehanizam za određivanje vremena koji kontrolira kada i koliko dugo vaša djeca mogu biti *online*, ključ koji sprječava pokretanje alternativnih pretraživača i mogućnost kreiranja popisa dopuštenih adresa e-pošte. No ova značajka radi samo ako se vaše dijete prijavi za rad sa svojim *online* identitetom. Najlakši način da se zaobiđu ova ograničenja je upotrijebiti vaše korisničko ime i lozinku. AOL nudi i uslugu KOL, koja je pokrenuta posebno zbog djece i obuhvaća sobe za čavrljanje koje nadzire osoblje AOL-a. Za ove se usluge morate pretplatiti.
- Earthlink nudi besplatne kontrole za roditelje sa svojim opcijama usluga dial-up i high-speed veza. Na vrhu popisa je filtriranje Web lokacija. Svoju djecu možete ograničiti na 15.000 lokacija koje odobrava Earthlink ili im možete dati potpuni pristup Internetu, osim za 3 milijuna lokacija koje Earthlink blokira u dijelu svojeg sustava kontrola za roditelje. Earthlink može i automatski ukloniti prostote s Web lokacija. Earthlink nudi i za djecu ugodan CyberFriends Communicator koji uključuje e-poštu, čavrljanje, oglasne ploče i IM funkcije. Roditelji mogu kreirati bijeli popis ljudi s kojima njihova djeca smiju komunicirati. Oni mogu i pregledavati cijelu e-poštu koju njihova djeca šalju i primaju preko CyberFriends Communicator. Na kraju, roditelji mogu ograničiti vrijeme koje djeca provode *online*. Kao što smo spomenuli, ove se kontrole mogu primijeniti samo ako se vaše dijete prijavi za rad pod vlastitim identitetom.
- Children's Internet je *online* usluga posvećena djeci. Ona zaključava radnu površinu kako bi djeca mogla koristiti samo značajke ugrađene u uslugu (to obuhvaća pretraživanje Weba, e-poštu i čavrljanje). Ako vaše dijete ima vlastito računalo, ovo bi moglo biti dobra opcija. Detalje potražite na adresi www.childrensinternet.com.

Kontrole spama

Veliki problem e-pošte je pornografskog sadržaja ili na drugi način loše, a vaša djeca ne mare za to da bi takav materijal mogao dospjeti u dječji poštanski sandučić za e-poštu. Rješenje za filtriranje spama može vam pomoći da isključite

pornografsku i seksualno eksplicitnu *junk* poštu iz poštanskih sandučića svoje djece. Detalje o rješavanju *spama* naći ćete u 6. poglavlju "Recite 'ne' *spamu*".

Dodatno, *spamere* koji šalju pornografsku *junk* e-poštu vašoj djeci možete prijaviti. Da biste poslali prijavu posjetite Web lokaciju za National Center for Missing and Exploited Children (www.missingkids.com). Kliknite vezu CyberTipline na lijevoj strani stranice, pomaknite se dolje po stranici do naslova Unsolicited Obscene Material Sent to a Child pa kliknite gumb Report. Vaš izvještaj možda neće rezultirati trenutnom istragom, ali ako se skupi dovoljan broj prijava, mogli biste pomoći da *spamer* završi u zatvoru.

8.2 Seksualni grabežljivci i Internet

Nesretna činjenica modernog života je ta da seksualni grabežljivci koriste Internet – naročito *online* sobe za čavrljanje – da bi pronašli potencijalne žrtve. Prema izvještaju iz 2000. godine Crimes Against Children Research Centera (Centar za istraživanje kriminala nad djecom), gotovo je jedan od pet mladih korisnika Interneta koji su bili uključeni u istraživanje primilo nepoželjne seksualne ponude. Još je više zabrinjavajuće to da je 3% ispitanika prijavilo primanje "agresivnih ponuda" za *offline* kontakt. Približno četvrtina djece kojima su poslane ponude bila je u dobi od 10 do 13 godina, dok je 77% bilo u dobi između 14 i 17 godina. (Za vezu do ovog izvještaja pogledajte odjeljak "Korisni izvori".)

Ovaj se problem pogoršava jer su djeca manje oprezna na Internetu nego što su u realnom svijetu, djelomice zato što Internet pruža lažan osjećaj anonimnosti i sigurnosti. Zato se djeca mogu ohrabriti te se upustiti u konverzaciju ili veze na koje inače ne biste pristali u osobnom kontaktu. Uz to, mlađa djeca podložna su manipulacijama i mogu razviti pogrešno povjerenje u *online* "prijatelje".

Ali prije nego što iščupate telefonsku žicu iz računala, mogli biste poduzeti korake da biste zaštitili svoju djecu dok su ona *online*. Prvo i osnovno je to da razgovarate s njima. Koristite jezik koji odgovara dobi djeteta da biste raspravili problem i ohrabrite ga da dođe k vama ako naiđe na Internetu na nešto što mu nije ugodno. Svakako držite dijete na oku dok je *online*. Kao što smo prije raspravili, možete učiniti i oboje: fizički nadzor i korištenje softvera nezavisnih proizvođača. Detaljno ćemo razmotriti problem neprikladnog kontakta i moguća rješenja u preostalom dijelu ovog odjeljka.

Sprječavanje nepoželjnih kontakata

Poznajući načine na koji grabežljivci rade moći ćete svojoj djeci bolje objasniti koji su znakovi opasnosti. A ako nadzirete *online* aktivnost svoje djece, odmah ćete prepoznati sumnjivu komunikaciju.

Prema FBI-ju seksualni grabežljivci se najvjerojatnije šuljaju po sobama za čavrljanje da bi uspostavili vezu s djecom. Otvorena priroda ovih soba olakšava započinjanje *online* konverzacije koja obično počinje bezazlenim razgovorima i popularnoj umjetnosti, glazbi i drugim temama koje su djeci zanimljive. S vremenom grabežljivci mogu uspostaviti vezu pružajući pažnju, naklonost, suosjećajnost i čak ponuditi darove. Kada zadobiju povjerenje djeteta, mogu započeti dodatni razgovor na privatnijem mediju kao što su e-pošta, instatnt poruke (instat messaging –IM; AOL, MSN, ICQ...) ili čak telefon. Tada se počinju uvoditi seksualne teme ili dijeliti eksplicitne materijale, uključujući dječju pornografiju. Grabežljivci mogu i pokušati dogovoriti sastanke s potencijalnim žrtvama; FBI izvještava da je bilo slučajeva kad je žrtva primila čak i avionske karte kako bi je ohrabrili za dolazak na sastanak.

Primamljivo je jednostavno zabraniti pristup sobama za čavrljanje, ali to nije realno rješenje s obzirom na velik pristup Internetu. Djeca mogu dospjeti *online* u školi, knjižnici, kod prijatelja, na javnim kioscima u Internet kafićima i kod kuće dok vi niste doma. Uz to IM i čavrljanje mogu biti dobri i korisni načini koji omogućuju djeci da komunikacijom stječu svoje društveno iskustvo. Zato, umjesto da povučete kočnicu, upotrijebite sljedeće savjete koji će vam pomoći da vaše kućno računalo bude sigurno i da naučite svoju djecu kako da postanu mudri korisnici Interneta:

- Razgovarajte sa svojom djecom o potencijalnim opasnostima na Internetu. Zamolite ih da vam kažu ako imaju bilo kakav kontakt koji im je neugodan. Ako niste sigurni kako započeti razgovor, posjetite lokaciju NetSmartz.org, koju sponzorira Center for Missing and Exploited Children (Centar za nestalu i zlostavljanu djecu). NetSmartz.org ima informacije o *online* sigurnosti za djecu i tinejdžere i odličan je izvor podataka za roditelje.
- Uputite svoju djecu da ne otkrivaju svoja imena, dob, adresu ili telefonske brojeve u sobama za čavrljanje, e-pošti, IM-u itd. Isto tako ne bi smjeli slati svoje fotografije *online*.
- Ako možete, postavite svoje kućno računalo u najprometniju sobu u kući, na primjer, u dnevni boravak. Nadzirite *online* aktivnost svoje djece, uključujući e-poštu i Web lokacije koje posjećuju.

- Pazite na znakove opasnosti, kao što je napomenuto u okviru "Znakovi po kojima možete otkriti da je vaše dijete u *online* opasnosti", na kraju ovog poglavlja.
- Iskoristite kontrolne značajke za roditelje koje su dostupne kod vašeg davatelja usluga, u pretraživačima i tražilicama te u softveru nezavisnih proizvođača.

Prijava seksualnih mamljenja

FBI preporučuje da prijavite dječju pornografiju, ako je dospjela u ruke bilo kojeg člana vaše obitelji, ako vaše dijete ispod 18 godina starosti netko mami na seks ili ako to dijete prima eksplicitne slike od nekoga koga poznaje a taj je također maloljetan.

Te zločine možete prijaviti lokalnom sudu ili policiji. Možete i upotrijebiti CyberTipline lociran na polaznoj stranici National Centera for Missing and Exploited Children na adresi www.missingkids.com da biste prijavili incident.

FBI također napominje da biste, ako se jedan od ovih scenarija dogodi, a vi ga prijavite, trebali isključiti svoje računalo i ne dirati ga. Nemojte brisati ili kopirati datoteke ili slike. Zakonski ovlaštene osobe odnijet će vaše računalo na forenzičnu obradu, što može potrajati nekoliko dana ili tjedana.

Softver za nadziranje Interneta

Uz razgovaranja sa svojom djecom o potencijalnim opasnostima softver za nadziranje Interneta može vam pomoći da postavite ograničenja i budno pratite *online* aktivnost svoje djece. Neki od vas bi se mogli kajati zbog špijuniranja vlastite djece dok surfaju Webom ili se bojati da ste bolesno opsjednuti njihovom sigurnošću. Drugi roditelji na to mogu gledati kao na odgovarajuću mjeru predostrožnosti, poput kacige za bicikl ili sigurnosnih pojaseva u automobilu. Kako daleko ćete ići u ograničavanju i nadziranju aktivnosti ovisit će o raznim faktorima, uključujući starost djece (starija djeca vjerojatnije će biti hrabrija i zaobići filtre postavljene u pretraživaču ili tražilici); na vama je da procijenite s kolikim se rizicima susreću; i koliko ste vremena, truda i novca voljni uložiti.

Odjeljak "Filtriranje nepoželjnog sadržaja" daje popis jednostavnih i besplatnih filtara. Ovaj odjeljak pregledava softver koji je dizajniran za postavljanje roditeljskih kontrola i pruža pogled na djetetovo korištenje Weba. Ova kategorija

softvera nudi opsežnije kontrole i veći skup značajki od opcija o kojima smo prije govorili, ali te ćete proširene mogućnosti morati platiti.

Kako valja birati?

Postoji nekoliko kriterija za odabir softvera za nadziranje Interneta. Prvi je opsežnost kontrola. Područja koja ćete najvjerojatnije željeti kontrolirati su pretraživanje Weba i *online* čavrljanje te IM programi. Dobar bi proizvod trebao obuhvaćati i problem pretraživanja po slikama u tražilicama, ili filtriranjem rezultata pretraživanja ili zaključavanjem korisnika u unaprijed provjerenu tražilicu koja ne vraća nepoželjne rezultate. Moglo bi vas zanimati i filtriranje te nadzor e-pošte.

Pri ocjenjivanju programa imajte na umu razlike između filtriranja i nadziranja. Filtriranje blokira nepoželjan sadržaj ili ga zamjenjuje X-evima ili točkama. Nadziranje vam omogućuje pregledavanje informacija da biste saznali što vaša djeca rade *online* (na primjer, pregledavanje Web lokacija koje su posjećivala ili snimanje cijele IM konverzacije).

I uz specifične kontrole trebali biste znati koje su različite metode filtriranja, naročito Web sadržaja. Najjednostavniji sustav je crna lista URL-a Web lokacija koje sadrže loš materijal ili ključnih riječi koje mogu ukazivati na takav materijal. Te crne liste uglavnom održavaju tvrtke koje proizvode softver za roditeljsku kontrolu. One vjerojatno pokrivaju raspon kategorija uključujući pornografiju, nasilje, konzumiranje droga i alkohola itd. Crne su liste efikasne ako su opsežne. No, s obzirom na veličinu i primamljivost Interneta, stalno se pojavljuju nove lokacije a stare nestaju. Zato, prilikom uspoređivanja proizvoda potražite sustave koji redovito ažuriraju svoje popise. Većina sustava omogućuje vam i da sami odredite zabranjene i dopuštene lokacije.

Druga opcija je skeniranje Web lokacije prije nego što se ona prikaže u pretraživaču. To skeniranje može tražiti prostote, postojanje slika i pokušaj procjene vrste slike (na primjer, istraživanjem slika po licima, oblicima i koži). Od proizvoda s popisa iz tablice 8.1, EnoLogic NetFilter Home koristi analizu slika za blokiranje pornografskih slika u realnom vremenu. Analiza slike korisna je za otkrivanje nepoželjnog sadržaja bez potrebe ponovnog sastavljanja crne liste, ali ona može blokirati bezazlene lokacije. Mogli biste potražiti rješenje koje će roditeljima omogućiti da odblokiraju i omoguće pristup lokacijama koje su pogreškom blokirane.

softvera nudi opsežnije kontrole i veći skup značajki od opcija o kojima smo prije govorili, ali te ćete proširene mogućnosti morati platiti.

Kako valja birati?

Postoji nekoliko kriterija za odabir softvera za nadziranje Interneta. Prvi je opsežnost kontrola. Područja koja ćete najvjerojatnije željeti kontrolirati su pretraživanje Weba i *online* čavrljanje te IM programi. Dobar bi proizvod trebao obuhvaćati i problem pretraživanja po slikama u tražilicama, ili filtriranjem rezultata pretraživanja ili zaključavanjem korisnika u unaprijed provjerenu tražilicu koja ne vraća nepoželjne rezultate. Moglo bi vas zanimati i filtriranje te nadzor e-pošte.

Pri ocjenjivanju programa imajte na umu razlike između filtriranja i nadziranja. Filtriranje blokira nepoželjan sadržaj ili ga zamjenjuje X-evima ili točkama. Nadziranje vam omogućuje pregledavanje informacija da biste saznali što vaša djeca rade *online* (na primjer, pregledavanje Web lokacija koje su posjećivala ili snimanje cijele IM konverzacije).

I uz specifične kontrole trebali biste znati koje su različite metode filtriranja, naročito Web sadržaja. Najjednostavniji sustav je crna lista URL-a Web lokacija koje sadrže loš materijal ili ključnih riječi koje mogu ukazivati na takav materijal. Te crne liste uglavnom održavaju tvrtke koje proizvode softver za roditeljsku kontrolu. One vjerojatno pokrivaju raspon kategorija uključujući pornografiju, nasilje, konzumiranje droga i alkohola itd. Crne su liste efikasne ako su opsežne. No, s obzirom na veličinu i primamljivost Interneta, stalno se pojavljuju nove lokacije a stare nestaju. Zato, prilikom uspoređivanja proizvoda potražite sustave koji redovito ažuriraju svoje popise. Većina sustava omogućuje vam i da sami odredite zabranjene i dopuštene lokacije.

Druga opcija je skeniranje Web lokacije prije nego što se ona prikaže u pretraživaču. To skeniranje može tražiti prostote, postojanje slika i pokušaj procjene vrste slike (na primjer, istraživanjem slika po licima, oblicima i koži). Od proizvoda s popisa iz tablice 8.1, EnoLogic NetFilter Home koristi analizu slika za blokiranje pornografskih slika u realnom vremenu. Analiza slike korisna je za otkrivanje nepoželjnog sadržaja bez potrebe ponovnog sastavljanja crne liste, ali ona može blokirati bezazlene lokacije. Mogli biste potražiti rješenje koje će roditeljima omogućiti da odblokiraju i omoguće pristup lokacijama koje su pogreškom blokirane.

Većina softvera za roditeljsku kontrolu omogućuje ograničavanje vremena koje vaše dijete može provoditi *online*, blokiranje ili filtriranje IM-a ili čavrljanja i sprječavanje programa da preuzimaju datoteke, te sprječavanje djece da ne upisuju osobne informacije poput telefonskog broja.

Neki sigurnosni programi isporučuju se s ograničenim roditeljskim kontrolama. Norton Internet Security, koji se sastoji od vatrozida, antivirusa, *anti-spywarea* i drugih važnih značajki obuhvaća i neke postavke Parental Controla za blokiranje pristupa nepoželjnom sadržaju. Kada se aktivira, može blokirati Web lokacije na temelju popisa kategorija koji održava Symantec, uključujući seks, golotinju, zlorabljenje droga i nasilje. Vi možete ograničiti korisnike na popis dopuštenih Web lokacija i sve ostalo blokirati. (Ovakva postavka može biti pretjerana, pogotovo za stariju djecu, kojoj će biti neprihvatljivo da joj je onemogućen pristup svakoj lokaciji koju će možda trebati.) Možete također blokirati određene programe za pristup Internetu i ograničiti novinske grupe.

Zamijetite da se svaki softver za roditeljsku kontrolu temelji na računima korisnika koji se kreiraju za svaku osobu koja koristi vaše računalo. Ako vaša djeca znaju korisnička imena i lozinke odraslih, mogu zaobići roditeljske kontrole (uz pretpostavku da odraslima dajete neograničen pristup). Neki proizvodi nude pritajene mehanizme pa vaša djeca neće vidjeti ikonu proizvoda na ekranu sustava. Pritajena postavka može biti korisna ako imate stariju djecu koja su vješta na računalu i koja bi mogla probati zaobići vaša ograničenja.

Proizvodi popisani u tablici 8.1 predstavljaju samo mali broj softverskih rješenja za roditeljsku kontrolu. Korisne recenzije softvera za roditeljske kontrole možete pronaći u *PC Magazineu* (www.pcmagazine.com) i na adresi http://internet-filter-review.toptenreviews.com/. Sredinom 2005. godine cijene za samostalan softver za roditeljske kontrole kretale su se u rasponu od 29,95 do 55 američkih dolara. Posebne ponude i rabati mogu utjecati na krajnju cijenu.

8.3 Pjesma od 3.000 USD i drugi problemi s dijeljenjem datoteka

Tema koja se stalno ponavlja u ovoj knjizi je da novac pokreće većinu sigurnosnih problema s kojima se suočavamo prilikom korištenja Interneta. O tome se radi i u ovom odjeljku, ali obrnutim redoslijedom: umjesto da ste vi žrtva Internet kriminalaca, dvije gigantske organizacije osjećaju da su *one* vaše žrtve, a *vi* ste lopovi. Pa, možda ne vi osobno, ali svatko tko koristi Internet da bi pronašao, preuzeo i dijelio glazbu i filmove zaštićene autorskim pravima bez plaćanja ijedne lipe za

Tablica 8.1

Odabrani softver za roditeljske kontrole

Proizvod	Proizvođač	Web lokacija	Značajke
ContentProtect	ContentWatch	www.contentwatch.com	Analiza web lokacija u stvarnom vremenu, blokiranje pristupa čavrljanju, vremenska ograničenja, dnevnik aktivnosti, zaštitna lozinka i drugo.
ContentWatch	SurfControl	www.cyberpatrol.com	Crne liste Web lokacija i bijele liste, analiza teksta na Web lokaciji u realnom vremenu, filtriranje rezultata pretraživanja u tražilicama, blokiranje čavrljanja i IM-a, vremenska ograničenja, blokiranje *spywarea* i drugo.
CYBERSitter	Solid Oak Software	www.cybersitter.com	Crne liste Web lokacija i bijele liste, blokiranje slika u tražilicama, vremenska ograničenja, snimanje IM konverzacije na AOL-u i u Yahoo! Messengeru, pritajeni mod i drugo.
EnoLogic NetFilter Home	EnoLogic	www.enologic.com	Analiza teksta i slika Web lokacija, korisničke crne liste, blokiranje čavrljanja, blokiranje unosa privatnih informacija, blokiranje prijenosa velikih datoteka, otkrivanje MP3 datoteka i drugo.
NetNanny	LookSmart	www.netnanny.com	Crne liste Web lokacija i bijele liste, dnevnik aktivnosti, filtriranje teksta u pretraživačima, čavrljanju, e-pošti i novinskim grupama, vremenska ograničenja, blokiranje pristupa čavrljanju i IM-u i drugo.

licencu ili tantijeme. Ove organizacije, Recording Industry Association of America (RIAA) i Motion Picture Association of America (MPAA), tvrde da su izgubile milijune dolara zbog tehnologije koja se naziva izravna razmjena datoteka.

Ova tehnologija radi ono što joj i samo ime kaže – dopušta korisnicima da razmjenjuju datoteke. Većina tih datoteka su glazbene datoteke, uglavnom u MP3 formatu, što je format za dešifriranje i sažimanje audio signala. Drugi popularni digitalni formati uključuju Windows Media Audio (WMA), koji koristi Microsoft i Advanced Audio Coding (AAC), koji koristi Appleov iTunes i iPod uređaji za reprodukciju. Programi za razmjenu datoteka omogućuju vam i da razmjenjujete druge vrste digitalnih datoteka kao što su filmovi, dokumenti, slike i softverski programi.

Općenito se razmjena datoteka odvija na mrežama za izravnu razmjenu datoteka (P2P mreže). P2P mreže sastoje se od individualnih čvorova koji su spojeni duž mreže. P2P mreže suprotnost su klijent/poslužitelj mrežama. Na klijent/poslužitelj mreži grupa klijenata šalje i prima podatke s centralnog poslužitelja. Taj poslužitelj može biti konfiguriran tako da dopušta klijentima da dijele iste datoteke ili resurse, ali klijenti ne komuniciraju individualno jedni s drugima; poslužitelj je glavno spremište informacija. Mreža u vašem uredu vjerojatno je izgrađena po modelu klijent/poslužitelj.

Nasuprot tome mreže za izravnu razmjenu datoteka nemaju glavni poslužitelj; svaki čvor ili sustav na mreži može preuzimati datoteke s drugih sustava i davati datoteke drugim sustavima. Veće P2P mreže imaju indeksirane čvorove koji govore koje su datoteke dostupne na kojem čvoru, a čvorovi se rangiraju prema svojem mrežnom kapacitetu.

Napster je prva P2P mreža koja je privukla pažnju javnosti. Ona je također jedna od prvih velikih P2P mreža koja se našla pod zakonskom paljbom produkcijske industrije. Ta je industrija tužila Napster za omogućavanje kršenja autorskih prava jer je mnogo ljudi koristilo Napster za preuzimanje i dijeljenje pjesama bez plaćanja. Napster je ugašen, ali se ponovno pojavio kao *online* glazbena prodavaonica koja plaća odgovarajuće tantijeme produkcijskoj industriji.

No, što se tiče razmjenjivanja datoteka i P2P mreža, dio digitalnog kolača opet je izvan torbe vlasnika. P2P mreže kao što su Kazaa, Grokster, Gnutella, Morpheus i stotine drugih omogućuju korisnicima da pronalaze, preuzimaju i dijele glazbeni, filmski i drugi digitalni sadržaj bez naknade.

Dakako, to ne sprječava RIAA od pokušavanja da vrati svoj dio kolača. Trenutno RIAA na svojoj strani nema tehnologiju; razni pokušaji šifriranja i zaštite digitalnog audio sadržaja na druge načine od kopiranja i distribuiranja nisu uspjeli. Međutim, RIAA ima zakon na svojoj strani: preuzimanje ili omogućavanje

preuzimanja sadržaja zaštićenog autorskim pravima bez dopuštenja nositelja autorskih prava je nezakonito. No, P2P softver je legalan, pa tu stvari postaju mnogo složenije.

RIAA i MPAA provode svoju pravnu bitku na dva fronta. Prvi, one progone proizvođače P2P softvera koji omogućavaju kršenje autorskih prava. Drugi, one progone organizacije (naročito sveučilišta) i pojedince koji ilegalno dijele sadržaj zaštićen autorskim pravima.

U travnju 2005. godine RIAA je objavila novi krug sudskih tužbi protiv pojedinaca koji su navodno krivi za ilegalno dijeljenje datoteka. Jedan bloger tvrdi da ovaj krug broji ukupno preko 10 000 ljudi koje je RIAA tužila (pogledajte http://share-nomore.blogspot.com/). 2003. godine RIAA je tužila stotine ljudi za ilegalno dijeljenje glazbe zaštićene autorskim pravima. Prosječna kazna iznosila je 3 000 američkih dolara.

MPAA također progone razmjenjivače datoteka. Ona je pokrenula početni krug sudskih tužbi u studenom 2004. godine, i nastavila s drugim krugom u siječnju 2005. godine.

U travnju 2005. godine predsjednik SAD-a, George W. Bush odobrio je prijedlog zakona i uveo novi zakon Family Entertainment and Copyright Act. Napisan protiv digitalnih pirata, zakon govori da će svatko koga se uhvati s predizdanjem filma, pjesme ili softverskog programa na svojem računalu biti optužen na do tri godine zatvora ili kaznama do 250 000 američkih dolara.

I konačno, Vrhovni je sud počeo slušati argumente u slučaju *MGM Studios, Inc. protiv Grokster, LTD* u rano proljeće 2005. godine. Bitan argument je taj da je MGM, filmski studio, tvrdio da je Grokster, P2P program za razmjenjivanje datoteka, kriv za sva kršenja autorskih prava jer je korisnicima pružio mehanizme za dijeljenje materijala zaštićenog autorskim pravima. Slučaj je složen i vjerojatno će uključiti veliku mjeru prosuđivanja prije nego što Sud donese vlastita pravila. Mnogi promatrači citiraju prethodan slučaj *Sony protiv Universal Studiosa*, u kojem je Universal tužio Sony za kršenje autorskih prava tvrdeći da je Sonyjeva Betamax tehnologija omogućila korisnicima da ilegalno kopiraju televizijske programe. Vrhovni sud presudio je u korist Sonyja, s obrazloženjem da Sony nije odgovaran za ono što njegovi korisnici rade s njegovom tehnologijom. Sud je također napomenuo da se potezi korisnika (snimanje TV emisija kako bi ih kasnije mogli pogledati) smatraju ispravnim korištenjem materijala zaštićenog autorskim pravima.

U trenutnom slučaju će ipak biti teško dokazati kako razmjena pjesama zaštićenih autorskim pravima među milijunima potencijalne publike predstavlja zakonski ispravno korištenje, uz značajan potencijalni gubitak prihoda koji trpi nositelj

autorskih prava. U vrijeme pisanja ovog poglavlja, Vrhovni sud nije se izjasnio u vezi s tim slučajem. Vezu do pregleda ovog slučaja i potencijalnih reperkusija potražite u odjeljku "Korisni izvori" na kraju ovog poglavlja.

Kako me mogu uloviti?

Internet pruža lažan osjećaj anonimnosti korisnicima P2P softvera. Kako broj sudskih tužbi koje su podnijele RIAA i MPAA pokazuje, individualni korisnici mogu se uhvatiti. Nije pitanje u tome mogu li one uloviti vas, već hoćete li biti među ljudima koju su uhvaćeni u njihovim gotovo već redovitim racijama u kojima traže kršitelje autorskih prava. Te organizacije trenutno traže najaktivnije korisnike, pa su šanse da vas pronađu male (uz pretpostavku da niste postavili Web poslužitelj koji "dila" digitalne audio datoteke).

Kako oni pronalaze kršitelje autorskih prava? Pa, najlogičniji način da se to učini je prijaviti se na razne P2P mreže i pronaći čvorove koji dijele sadržaj zaštićen autorskim pravima. RIAA i MPAA imaju vlastite kriterije prema kojima odlučuju koje čvorove progoniti, ali kad jednom odluče, one potvrde da taj čvor ilegalno drži autorski materijal. Potom mogu otkriti IP adresu čvora pomoću raznih lookup alata. Kada dođu do IP adrese, mogu otkriti tko je davatelj usluge tog čvora. Tada jednostavno podnose sudsku tužbu protiv "Nepoznatog počinitelja". Prema informacijama na lokaciji RIAA-e, tužitelji mogu podnijeti takvu tužbu kada ne znaju ime osobe koju tuže. Nakon podnošenja tužbe, tužitelj može uručiti sudski poziv ISP-u da bi dobio ime osobe koja koristi pronađenu IP adresu. Detaljne informacije možete pronaći na stranici www.riaa.com/news/newsletter/012104_faq.asp.

U svojim prijašnjim tužbama RIAA je pokušala provesti ovaj postupak na drugi način; odnosno, pokušala je ISP sudski prisiliti da navede ime i osobne informacije kršitelja autorskih prava kako bi potom mogla tužiti samo tu osobu. No, Verizon Online odbio je zahtjev RIAA-e. Tada je RIAA tužila Verizon, pa je slučaj dospio do Vrhovnog suda, koji je potvrdio presudu da davatelji usluga mogu tajiti identitet svojih klijenata. Međutim, proces s tužbom protiv "Nepoznate osobe" je u potpunosti legalan, što znači da ako se ISP-u uruči sudski poziv u tom procesu, on mora otkriti ime i osobne podatke svojeg pretplatnika.

Problemi sigurnosti kod P2P mreža

Uz potencijalne zakonske probleme koji proizlaze iz neplaćanja glazbe i filmova, P2P programi mogu vas izložiti sigurnosnim rizicima. Kada preuzmete i pokrenete koristiti neki P2P softver, možda nećete shvatiti da svoje računalo izlažete drugim

računalima na Internetu. Određena mapa koja sadrži digitalne datoteke za dijeljenje može biti otvorena Internetu. Nije li ispravno konfiguriran, mogli biste cijeli svoj tvrdi disk sa svim sadržajem otvoriti Internetu. Ako koristite vatrozid (a ako ste došli ovako daleko čitajući ovu knjigu, tada biste trebali imati instaliran vatrozid), trebat ćete otvoriti portove da biste omogućili funkcioniranje P2P softvera. Međutim, otvaranjem tih portova izlažete svoje računalo opakim provalnicima.

Uz to, prema raspravi iz 6. poglavlja, većina P2P aplikacija može uključivati *adware* koji može pratiti vaše *online* ponašanje, generirati dosadne iskočne oglase i narušiti performanse vašeg računala. A na kraju, napadači i kriminalci počeli su postavljati trojanske konje i drugi *malware* u P2P datoteke dodjeljujući im zanimljiva imena. Mislite da ste dobili super B stranu ploče grupe U2 ili kopiju filma *Hitchhiker's Guide to the Galaxy*, ali umjesto toga instalirali ste keystroke logger na svoje računalo.

Ako ipak želite koristiti P2P softver, svakako koristite antivirusni i *anti-spyware* softver za skeniranje datoteka koje preuzimate, i pažljivo čitajte upute za konfiguriranje da biste osigurali kako će datoteke koje izlažete Internetu biti samo one koje zaista želite dijeliti. Kao što je već spomenuto P2P programi postavljaju posebnu mapu na računalu za tu svrhu.

Legalno ili ilegalno?

Jeste li zbunjeni cijelom ovom zakonskom zavrzlamom oko dijeljenja datoteka? Tablica 8.2 je brzi vodič koji će vam pomoći da shvatite što je ispravno i zbog čega biste možda mogli dobiti tužbu.

Tablica 8.2

Legalno nasuprot ilegalnom dijeljenju datoteka

Legalno	Ilegalno
Korištenje P2P softvera	Korištenje P2P softvera za preuzimanje i dijeljenje autorskog materijala bez dozvole nositelja autorskih prava
Kupovanje glazbe *online*	Kupovanje glazbe *online* i potom dijeljenje te glazbe preko P2P softvera
Kopiranje digitalnih audio ili video datoteka koje ste platili na CD ili prijenosni uređaj za reprodukciju	Kopiranje digitalnih audio ili video datoteka za daljnje preprodavanje ili dijeljenje na P2P mrežama

8.4 Popis za provjeru

Upotrijebite ovaj popis za provjeru kao brzi referentni vodič kroz gradivo izneseno u ovom poglavlju.

Učinite

- Iskoristite opcije filtriranja za uklanjanje lošeg sadržaja s Interneta.
- Pokušajte ograničiti djecu prilikom korištenja Interneta na računalo koje je smješteno u najprometnijoj sobi kao što je dnevni boravak ili kuhinja.
- Razgovarajte sa svojom djecom o potencijalnim opasnostima koje vrebaju na Internetu.
- Uvjerite svoju djecu da ne šalju svoja imena, slike, telefonske brojeve, adrese i adrese e-pošte na Web.
- Pratite znakove da je vašoj djeci pristupio seksualni napasnik *online*.
- Razgovarajte sa svojom djecom o zakonskim i sigurnosnim problemima vezanim uz dijeljenje datoteka u sustavinma za izravnu razmjenu datoteka.

Nemojte učiniti

- Nemojte pustiti djecu da bez nadzora koriste Internet.
- Nemojte vjerovati da su sustavi za filtriranje 100% efikasni.
- Nemojte vjerovati da se vaš sustav za filtriranje ne može zaobići.

8.5 Korisni izvori

Ovaj odjeljak daje popis dodatnih izvora koji će vam pomoći da saznate više.

National Center for Missing and Exploited Children je neprofitna organizacija koja pruža usluge obiteljima nestale, zlostavljane ili seksualno iskorištavane djece. Web lokacija Centera, www.missingkids.com, sadrži mnogo informacija o *online* zaštiti djece. Isto tako, ako trebate prijaviti seksualno mamljenje ili druge probleme, CyberTipline lokacije odlično je mjesto za početak. Veza do CyberTiplinea nalazi se na lijevoj strani polazne stranice

www.missingkids.com koji je objavio Crimes Against Children Research Center, posjetite stranicu www.missingkids.com/en_US/publications/NC62.pdf.

Detaljne informacije o tome kako razgovarati s malom djecom ili tinejdžerima o *online* sigurnosti naći ćete na adresi www.netsmartz.org. Mlađa djeca mogu pregledati i lokaciju www.netsmartzkids.org site gdje se nalazi *online* priručnik o sigurnosti na Internetu. NetSmartz sponzoriraju National Center for Missing and Exploited Children i Boys and Girls Clubs of America.

"A Parent's Guide to Internet Safety" koji je objavio FBI, sadrži korisne savjete kako djecu *online* zaštititi. U tom su vodiču navedeni i koraci koje treba poduzeti ako sumnjate da vaše dijete komunicira sa seksualnim napasnikom. Vodič se nalazi na adresi www.fbi.gov/publications/pguide/pguidee.htm.

Detalje o glazbenom piratstvu iz perspektive Recording Industry Association of America (RIAA) naći ćete na stranici www.riaa.com/issues/piracy/default.asp. Možda ćete htjeti provjeriti vezu Penalties (kazne) u gornjem desnom kutu stranice.

Julie Hilden napisala je sjajan pregled sudskog slučaja *MGM protiv Grokstera* prije Vrhovnog suda. Možete ga pročitati na stranici www.cnn.com/2005/LAW/02/16/hilden.fileswap/.

Znakovi koji ukazuju da bi vaša djeca mogla biti u *online* opasnosti

Unatoč brizi, ipak je moguće da vaša djeca naiđu na *online* seksualne grabežljivce ili uznemirujući seksualni materijal. FBI je istaknuo sedam znakova koji mogu upućivati na to da je vaše dijete izloženo *online* riziku. Tih sedam znakova koji su ovdje popisani preneseni su iz vodiča FBI-ja "A Parent's Guide to Internet Safety". Vezu do cijelog vodiča naći ćete u odjeljku "Korisni izvori". Iako su ovi znakovi korisni, roditelji bi trebali imati na umu da dva od ovih znakova (provođenje mnogo vremena na Internetu i izoliranje od obitelji) mogu biti potpuno normalno ponašanje tinejdžera. Ako sumnjate da postoji problem, porazgovarajte sa svojim djetetom prije donošenja zaključaka.

- Vaše dijete provodi mnogo vremena na Internetu. Koliko je to "mnogo" varira od obitelji do obitelji, pa to morate sami procijeniti. Međutim, FBI tvrdi da su grabežljivci djece najaktivniji navečer ili tijekom vikenda.

nastavlja se...

- Pronalazite pornografiju na računalu svojeg djeteta. Seksualni grabežljivci mogu koristiti pornografiju, uključujući i dječju pornografiju da s djecom započnu diskusiju o seksu ili da zavedu potencijalne žrtve. Ako otkrijete da je netko vašem djetetu poslao pornografiju (naročito dječju), trebali biste kontaktirati lokalno tužiteljstvo. Možete i upotrijebiti CyberTipline koji se nalazi na lijevoj strani polazne stranice na adresi www.missingkids.com da biste prijavili incident. Ako lokalnom tužiteljstvu prijavljujete pornografiju, FBI preporučuje da isključite i ne dirate računalo. Možda će ovlaštena osoba iz tužiteljstva provesti forenzičku istragu pa će vam zato uzeti računalo.
- Vaše dijete nazivaju stranci ili ono naziva nepoznate brojeve. Seksualni grabežljivci često pokušavaju preseliti komunikaciju iz soba za čavrljanje na privatniji medij. Neki pokušavaju uvući djecu u seks telefonom i nagovoriti ih na sastanak uživo.
- Stranac šalje vašem djetetu poštu, darove ili pakete. Seksualni grabežljivci mogu provoditi dodatnu komunikaciju i koristiti darove da bi zadobili povjerenje.
- Vaše dijete brzo isključuje računalo ili se prebacuje na drugi ekran čim uđete u sobu. To je znak da dijete možda gleda nešto što vi ne biste željeli da vidi.
- Vaše se dijete povlači iz obitelji. Seksualni grabežljivac može ga pokušati izolirati od ostatka obitelji da bi omogućio manipuliranje vezom s djetetom. U najgorem slučaju, to može biti znak da je vaše dijete već postalo žrtva.
- Vaše dijete koristi alternativne *online* račune. Dok možete imati pristup primarnom *online* računu svojeg djeteta, ono može nevjerojatno lako postaviti račune e-pošte i IM-a o kojima ništa ne znate. Ti odvojeni računi mogu biti benigni, ali se mogu koristiti i za privatnu komunikaciju između grabežljivca i potencijalne žrtve.

9. poglavlje

Bežična i VoIP sigurnost

Nekad su računala bila računala, a telefoni su bili telefoni. Danas je stvarno teško razdvojiti ove dvije stvari, a u roku od pet godina to će biti potpuno besmisleno. Zahvaljujući razvoju bežičnog računalstva i Internet telefonije današnja računala su mobilnija nego ikada, pa telefonski poziv možete uputiti sa svojeg računala. U međuvremenu mobiteli, osobni digitalni pomoćnici (*personal digital assistants* – PDA-i) i bežični uređaji za e-poštu počinju sadržavati značajke, funkcije i moć procesiranja stolnih računala.

Taj razvoj ima mnogo dobrih strana. Bežična tehnologija nudi nevjerojatnu mobilnost i praktičnost kod kuće i olakšava spajanje na Internet izvan kuće. Za sada je bežično računalstvo ograničeno na nekoliko javnih pristupnih točaka. S vremenom ćete moći uživati u istoj vrsti raširene bežične Internet pokrivenosti koju dobivate od svojeg operatera mobilne mreže. Glas preko IP-a (*Voice over IP* – VoIP) trenutno pruža jeftinu uslugu telefoniranja pretvaranjem vašeg računala u telefon i usmjeravanjem vaših telefonskih poziva preko Interneta.

A kad smo kod telefona, mobilne verzije također prolaze kroz fantastične faze razvoja kako proizvođači dodaju značajke i usluge kao što su SMS poruke (tko bi mislio da će slanje tekstualnih poruka telefonom postati tako popularno?), digitalne fotografije i pristup Internetu. Uz to, uređaji poput BlackBerryja, koji omogućuje bežičnu e-poštu na putu i Palm Piloti, koji su digitalni rokovnici, obuhvaćat će i značajke telefona, čime će još više blijedjeti granica između

komunikacijskih uređaja koje držite u ruci. A u budućnosti (barem onoj o kojoj sanjaju oglašivači) lokalne će tvrtke emitirati prodajne ponude na vašim mobilnim telefonima dok budete prolazili pokraj njihovih prodavaonica.

Naravno, kako ste već do sada trebali pogoditi, dobre se strane svake tehnologije moraju usporediti s onima koje predstavljaju potencijalne nedostatke što se sigurnosti tiče. A nedostaci su, naročito u slučaju bežične tehnologije, veliki. Problemi idu u rasponu od bežičnih "nametnika" koji se zakvače na vašu vezu s Internetom i besplatno surfaju do lopova i drugih kriminalaca koji kradu osjetljive informacije. Kako se mobiteli budu pretvarali u dlanovnike, tako će imati sve više istih problema koji sada haraju PC-ima (virusi mobilnih telefona već postoje). A kada se vaše računalo pretvara u telefon preko VoIP-a, ta transformacija ima vlastitih mana, od koji neke imaju sigurnosne implikacije (94 ili 92 usluge). Ovo poglavlje govori o potencijalnim opasnostima ovih novih tehnologija i pomaže vam da te tehnologije šti je najbolje moguće iskoristite.

9.1 Kako radi bežična mreža?

Danas mnoga kućanstva imaju nekoliko računala i nekoliko osoba koje istodobno žele pristupiti Internetu. Zato se kućne mreže šire diljem domova u cijelom svijetu. Kućna mreža povezuje nekoliko računala da bi mogla razmjenjivati datoteke i dijeliti pristup Internetu. Kućne mreže mogu biti ožičene ili bežične. Bežične su mreže popularne jer vam nisu potrebni kabeli do svakog računala u kući, a vaša obitelj može istodobno dijeliti vezu s Internetom iz spavaćih soba, dnevnog boravka, radne sobe pa čak i iz vrta (ovisno o jačini pristupne točke).

Osnovna bežična veza zahtijeva dvije komponente: bežičnu karticu ili čip u računalu i pristupnu točku, koja se još naziva i bežični usmjerivač. Većina se današnjih prijenosnih računala isporučuje s mogućnosti bežičnog umrežavanja. Pristupna točka povezuje svaki mehanizma koji koristite za spajanje na Internet: telefonsku utičnicu, DSL modem ili kabelski modem. Više se računala može povezati preko radiovalova s jednom pristupnom točkom. Glavni proizvođači kućnih bežičnih mreža su Linksys, Belkin, D-Link i NetGear.

Današnje bežične kućne mreže temelje se na skupu standarda koji se zajednički nazivaju Wi-Fi, što je kratica od *wireless fidelity* (bežična odanost). Wi-Fi-jem upravlja Institute of Electrical and Electronics Engineers (IEEE), koji dijelom nadgleda tehnološke standarde da bi osigurao međudjelovanje proizvoda različitih proizvođača. Wi-Fi sadrži brojne standarde koji su opisani pomoću numeričkog sustava koji se naziva 802.11, što je naziv odbora koji kreira

standarde za bežične mreže. U ovom ćemo se poglavlju pozabaviti s četiri standarda: b, g, i a standardi odnose se na osnovna pitanja o prijenosu podataka. 802.1x opisuje radni okvir za razmjenu informacije za provjeru valjanosti između uređaja u bežičnoj mreži. Više o standardu 802.1x govorimo poslije u ovom poglavlju.

Standardi b, g i a razlikuju se na nekoliko načina, uključujući kapacitet (koja se količina podataka može prenijeti pri kojoj brzini), dometu (kako daleko signal može putovati), koji dio radio spektra koriste i kako rješavaju probleme interferencije. (Radio signali trpe interferenciju od fizičkih objekata kao što su zidovi, grede i prirodne tvorevine poput brda, te od elektromagnetskih valova koje generiraju drugi uređaji kao što su mikrovalne pećnice.)

Standard 802.11b je najrasprostranjeniji, što znači da većina bežične opreme koji kupujete koristi ili podržava ovaj standard. To također znači da mnoga javna mjesta poput kafića koriste taj standard. 802.11b ima maksimalan kapacitet od 11 megabita u sekundi i može slati i primati podatke na udaljenosti do 50 metara. Međutim, noviji standardi nude veću brzinu – do 54 megabita u sekundi – ali ih sada ne podržava mnogo proizvoda (činjenica koja će se brzo promijeniti). Novi se proizvodi stalno pojavljuju, a neki podržavaju višestruke standarde i mogu se prebacivati s jednog na drugi, ovisno o zahtjevima mreže. Odabir standarda znači prihvaćanje raznih ustupaka. Na primjer, 802.11a ima samo pola raspona drugih standarda, ali radi u 5 GHz spektru, koji je manje napučen i zato manje podložan elektromagnetskoj interferenciji. 802.11b i g imaju veće brzine i dostupni su u mnogim potrošačkim Wi-Fi proizvodima i javnim bežičnim mrežama. Međutim, može doći do interferencije iz bežičnih telefona i mikrovalnih pećnica. Tablica 9.1 sadrži informacije o tri Wi-Fi standarda.

9.2 Sigurnosti kod kućnih WLAN-ova

Praktičnost Wi-Fi mreža (koje se nazivaju i Wireless Local Area Networks ili WLAN-ovi, odnosno bežične lokalne mreže) ima svoju cijenu: ozbiljno naruša-vanje privatnosti i sigurnosti. To možda niste shvatili, ali bežična kartica ili čip u vašem računalu i vaša pristupna točka su zapravo radio prijemnici, doduše mali koji koriste različite frekvencije od tradicionalne AM/FM vrste. Signale koje šalju vaši bežični uređaji može uloviti bilo koji uređaj unutar dometa, a ne samo vaša pristupna točka. Napadači to znaju, pa koriste softverske programe koji se nazivaju sniferi i koji im omogućuju "prisluškivanje" nešifrirane bežične veze. Ovi sniferi su bežični ekvivalenti prislušnih uređaja na telefonskim linijama, osim što

Tablica 9.1

Standardni za bežične mreže

Standard	Maksimalna brzina	Domet	Podrška proizvoda	Frekvencija
802.11b	11 megabita u sekundi	30 do 50 metara	Najrasprostranjenija podrška među bežičnim proizvodima.	2.4 GHz
802.11g	54 megabita u sekundi	30 do 50 metara	Rastuća podrška među proizvodima. Unatrag je kompatibilan sa standardom 802.11b (iako pri brzini od 11 megabita u sekundi).	2.4 GHz
802.11a	54 megabita u sekundi	10 do 20 metara	Nova tehnologija koju podržava najmanje proizvoda (do sada). Ne radi sa standardima 802.11b ili g.	5 GHz

oni mogu ugrabiti e-poštu, vaše poruke prilikom dopisivanja pomoću IM-a i naravno svaku lozinku ili brojeve računa koje koristite tijekom bežične sesije. Bežični sniferski alati ažurirane su verzije žičanih sniferskih alata, koji mogu nadzirati prijenos na ožičenim mrežama. Međutim, bežične je snifere mnogo lakše koristiti jer se ne trebate spajati na žicu ni tražiti praznu mrežnu utičnicu – jednostavno ga uključite blizu neke Wi-Fi mreže i pratite protok prometa.

Uz snifere, svako drugo računalo s bežičnom karticom ili čipom u dometu može se spajati na vašu pristupnu točku. Većina WLAN tehnologije ima maksimalan domet od 50 matara, pa vaš signal ne putuje do Kine i natrag, ali zasigurno putuje dovoljno daleko za vaše susjede ili nekoga tko sjedi ispred vaše kuće da ga pokupi. Imajte na umu i to da bežični prijenos ne putuje pravocrtno; on se penje, spušta i zaobilazi poput trodimenzionalnih valova na vodenoj površini.

No da ne bi bilo nesporazuma, rizici kojima se izlažete korištenjem kućnog WLAN-a nisu toliko strašni. Šanse da će neki kriminalac visiti ispred vaših vrata u pokušaju da ugrabi vaš bežični promet vrlo su male. (Šanse da se to dogodi na nekom javnom mjestu mnogo su veće, ali o tome poslije.) Ono što bi se najvjerojatnije moglo dogoditi je to da bi neki znatiželjni susjed mogao gledati vaš promet ili besplatno koristiti Internet vezu. Također, neki bi se entuzijast za

bežičnu tehnologiju mogao provozati po vašem kvartu koristeći poseban softver za traženje bežičnih mreža. To se zove *war driving* (što je igra riječi iz pojma "war dialing" – napadačka tehnika s automatiziranim računalnim programom koji poziva telefonske brojeve s dugačkog popisa u potrazi za računalnim modemima). War driveri mogli bi tražiti besplatan pristup Internetu u svojem susjedstvu, ali neki od njih traže način da provale u mreže. No, njih će vjerojatnije privući korporativni WLAN-ovi od kojih mnogi imaju oskudnu ili nikakvu zaštitu.

Dok neki ljudi svoj pristupne točke drže otvorenima da prošire pristup Internetu, ako vam je draža privatnosti, svoj WLAN možete zaključati. Najprije iskoristite mehanizme šifriranja koji su dostupni s točkama pristupa. Šifriranje uzima podatke koje šaljete sa svojeg računala na pristupnu točku (i obratno) i pretvara ih u nečitki tekst. To sprječava druge korisnike da pregledaju sve što šaljete i primate na svojoj bežičnoj vezi.

Postoje tri glavna mehanizma za šifriranje WLAN prometa: WEP *(Wired Equivalent Privacy)*, WPA *(Wi-Fi Protected Access)* i WPA2 (ažurirana verzija WPA koja koristi jači algoritam za šifriranje). WPA2 specifikacija međudjelovanja za 802.11i, još jedan bežični standard kojemu je cilj poboljšanje sigurnosti bežičnih mreža.

WEP se pojavio s prijašnjim verzijama bežičnih mreža i pokazao se gotovo univerzalno beskorisnim, naročito za osiguravanje rada WLAN-ova. Najveći problem kod WEP-a je njegovo slabo korištenje tehnologije šifriranja; odnosno, on koristi kratke ključeve šifri tijekom dugog vremenskog razdoblja. Ključ je matematička funkcija koja pretvara običan tekst u šifrirani tekst i potom ga ponovno vraća u običan tekst. Ključevi mogu biti raznih duljina, od 40 do 2048 bita i dulji. Općenito govoreći, što je ključ dulji, teže će računalo dešifrirati šifriranu poruku isprobavanjem svake moguće kombinacije brojki i slova. No, dugi ključevi zahtijevaju i jaču snagu obrade za provođenje funkcija šifriranja i dešifriranja, pa se kraći ključevi koriste kao ustupak za brzinu obrade. Neki programi koji koriste kratke ključeve, brzo te ključeve mijenjaju (recimo svake minute) pa dok napadač probije jedan ključ, morat će početi iznova kada novi ključ proradi.

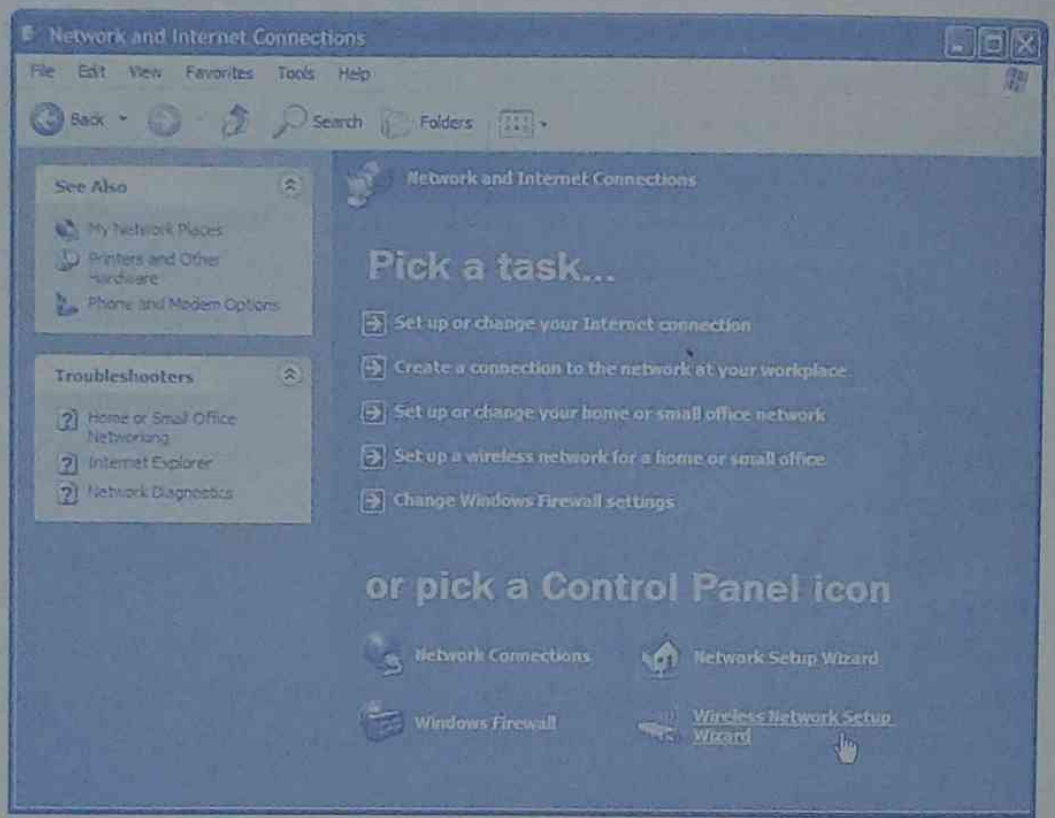
Zbog toga što je WEP koristio kratke ključeve tijekom dugačkih vremenskih razdoblja, i slabo je ključeve implementirao, istraživači su ubrzo otkrili da uz malo vremena i pomoći računala napadač može dešifrirati WEP-šifrirane prijenose. Brzo su se na Internetu pojavili softverski alati za napadanje WLAN-ova. Najozloglašeniji, poznat kao AirSnort, razbija WEP-zaštićene transmisije za nekoliko minuta.

WPA i WPA2 rješavaju nedostatak WEP-a korištenjem duljih ključeva i njihovim češćim mijenjanjem. Ako danas imate bežičnu pristupnu točku, ona koristi WPA

ili WPA2; starija WLAN oprema možda će zahtijevati nadogradnju s WEP-a na WPA. Ako nadogradnja nije dostupna, i dalje biste trebali koristiti WEP, jer je nekakva zaštita bolja od nikakve. (WEP je beskoristan kod korporativnih mreža, koje će vjerojatnije biti mete kriminalaca i imaju mnogo osjetljivih informacija koje njima kolaju. No, WEP je dovoljan da vašim susjedima ne dopusti njuškanje po vašem bežičnom prometu.)

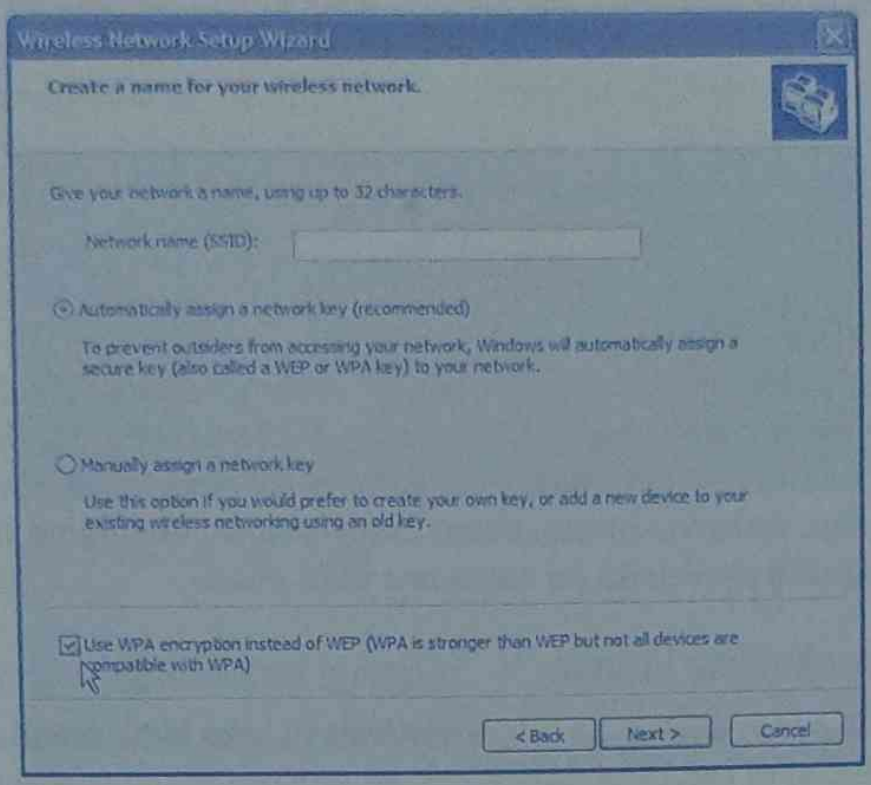
WPA i WPA2 imaju različite modove za tvrtke i kućne korisnike. Kućni bi korisnici trebali odabrati opciju WPA-PSK *(Wi-Fi Protected Access Preshared Key)* pri postavljanju bežične pristupne točke. WPA-PSK zahtijeva da postavite frazu za prolaz koju pristupna točka koristi za generiranje šifriranog ključa. Dobra fraza za prolaz sastoji se od brojki i slova. Frazu za prolaz unosite u svaki uređaj koji želite povezati s pristupnom točkom. Kada je WPA u pogonu, cijela komunikacija između vašeg računala i pristupne točke je šifrirana.

Windows XP Service Pack 2 (SP2) ima Wireless Network Setup Wizard koji vam pomaže prilikom konfiguriranja WLAN-a. Da biste pronašli tog čarobnjaka kliknite Start, odaberite Control Panel i Network and Internet Connections. Wireless Network Setup Wizard nalazi se uz ikonu bežične kartice, kao što je prikazano na slici 9.1.



Slika 9.1 Pristupanje Wireless Network Setup Wizardu

Čarobnjak vas vodi kroz sve korake koji su potrebni za kreiranje sigurne bežične mreže. Prvi ekran traži da odaberete neki SSID (o čemu govorimo poslije u ovom odjeljku), ka što je prikazano na slici 9.2. On vas pita i želite li automatsko ili ručno dodjeljivanje mrežnog ključa. To je ključ šifriranja koji štiti vašu komunikaciju. Microsoft preporučuje automatsku postavku. Ako vaša pristupna točka podržava WPA, potvrdite okvir na dnu ekrana da biste koristili WPA umjesto WEP šifriranja.



Slika 9.2 Biranje SSID-a i WPA-a

Uz šifriranje, drugi mehanizam zaštite za bežične mreže je 802.1x. Taj standard je radni okvir za slanje informacija za provjeru valjanosti, kao što su lozinke, digitalni certifikati ili sigurnosni tokeni, da biste dobili pristup nekoj bežičnoj mreži. Kada postavljate kućnu mrežu ne trebate brinuti o standardu 802.1x ali na njega biste mogli naići ako pristupate javnoj bežičnoj mreži kao što je ona u kafiću ili u hotelu.

Da biste osigurali svoju Wi-Fi mrežu, možete poduzeti i dodatne korake o kojima govorimo u sljedećim odjeljcima.

Promjena osnovnog SSID-a

SSID *(Service Set Identifier* – Identifikator uslužnog skupa) je 32-znakovni identifikator za bežičnu pristupnu točku. SSID u osnovi djeluje kao ime mreže da biste svoju pristupnu točku i WLAN mogli razlikovati od ostalih pristupnih točaka. Svaki uređaj koji se želi povezati na vašu pristupnu točku mora znati SSID. Problem je u tome što većina proizvođača isporučuje iz tvornice pristupne točke s istim osnovnim SSID-om (na primjer, "default"). Ti tvornički SSID-ovi dobro su poznati, pa ih trebate promijeniti. Za SSID možete odabrati ime po želji, ali je najbolje koristiti kombinaciju brojki i slova. SSID-ovi se uglavnom šalju preko etera nešifrirani, pa nemojte koristiti osjetljive informacije kao što je datum vašeg rođenja, lozinke s Interneta, ime ili adresu. Promijenite li SSID na svojoj pristupnoj točki, trebat ćete ga unijeti na svakom računalu za koje želite da koristi tu pristupnu točku.

Isključite emitiranje

Vaša pristupna točka može biti konfigurirana tako da emitira svoj SSID u redovitim vremenskim intervalima (recimo, svakih nekoliko sekundi). To je korisna značajka za velike WLAN-ove na kojima se korisnici mogu seliti s jedne na drugu pristupnu točku. Za kućnu mrežu, trebali biste isključiti emitiranje kako biste spriječili mogućeg provalnika da sazna ime vaše mreže.

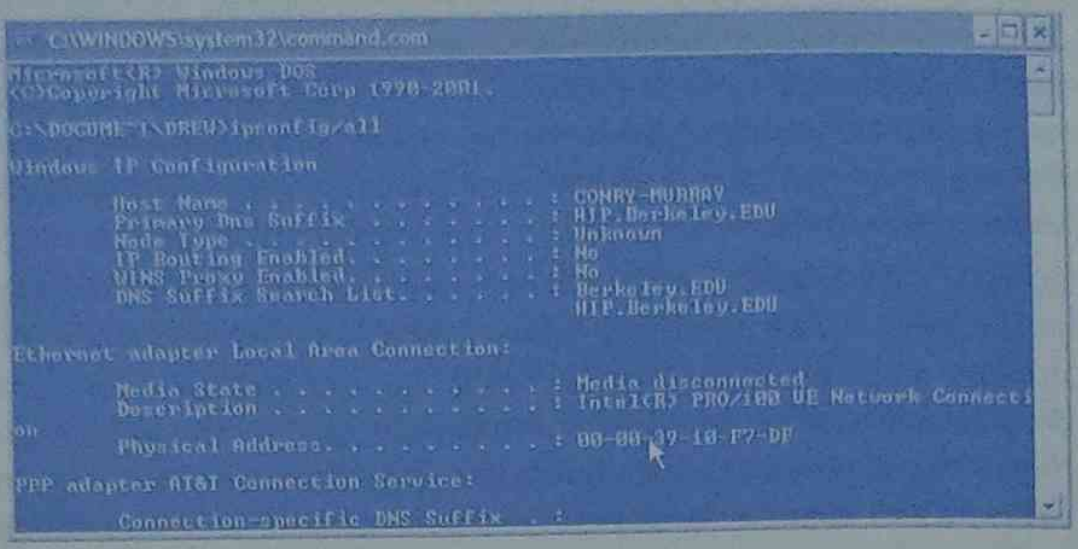
Promijenite osnovne lozinke

Pristupne točke mogu tražiti da odaberete lozinku kako biste mogli mijenjati postavke. Međutim, kao i kod SSID-a, mnogi proizvođači isporučuju pristupne točke s osnovnim lozinkama Te su lozinke dobro poznate kriminalcima, tako da je u vašem najboljem interesu da ih promijenite.

Uključite MAC filtriranje

Neke vam pristupne točke omogućuju da ih konfigurirate tako da se samo računala sa specifičnim MAC adresama mogu na njih spajati. (MAC adresa nema nikakve veze s Macintosh računalima, koja se skraćeno nazivaju Macovi. MAC je kratica od Media Access Control, što znači kontrola pristupa medija.) MAC adresa je jedinstveni broj koji se dodjeljuje svakoj kartici mrežnog sučelja *(Network Interface Card* – NIC) – ne postoje dva NIC-a s istim brojem. NIC, koji se ponekad naziva i Ethernet kartica, koristi se za spajanje računala na računalne mreže. Većina prodanih računala u posljednjih nekoliko godina imaju NIC. Budući da je svaka MAC adresa jedinstvena, MAC filtriranje je efikasan način blokiranja pristupa nepoznatih računala vašem WLAN-u.

Da biste pronašli MAC adresu kliknite gumb Start, odaberite Run i upišite command. To otvara DOS prozor s treptajućim C promptom. Iza C prompta upišite ipconfig/all i pritisnite Enter. Računalo vraća popis vlastitih specifikacija kao što se vidi na slici 9.3. Potražite unos Physical Address. To je vaša MAC adresa. MAC adresa koristi brojke i slova i izgleda slično ovome: 00.0D.60.FE.0F.1B. Ako vaše računalo nema NIC, tada ne možete koristiti MAC filtriranje.



Slika 9.3 MAC adresa računala

Sigurnosni softver za bežične sustave

Ako ste aktivirali pristupnu točku i pratili korake za osiguravanje svoje bežične veze, tada ste vjerojatno već sigurniji od većine ljudi oko vas. To je dobro jer kriminalci s Interneta naginju oportunizmu: prvo kreću na nezaštićene mete.

No, ako želite dodatnu sigurnosti, tada biste trebali kupiti programe za bežičnu zaštitu. Prava vrijednost tih dodatnih programa je pomoć koju vam nude kada se spajate na druge bežične mreže, kao što je ona u kafiću ili hotelu.

Proizvođač sigurnosnog softvera McAfee nudi besplatno skeniranje da bi provjerio sigurnost veze bežične mreže koju koristite. Test na vaše računalo učitava ActiveX kontrolu da bi mogao provesti provjeru, pa morate koristiti pretraživač Internet Explorer da biste pokrenuli provjeru. Za testiranje otiđite na www.mcafee.com. Kliknite sekciju za kućne korisnike i u sekciji Free Services potražite McAfee Wi-Fi Scan.

Trend Micro, obuhvaća osobni vatrozid, antivirusni softver i *anti-spyware* softver. Modul Wi-Fi Intrusion Detection upozorava kada neki *war driver* ili nepoznati korisnik ulazi u vašu bežičnu mrežu. Posjetite lokaciju www.trendmicro.com.

Tvrtka pod imenom OTO proizvodi Wi-Fi Defense 1.0, što je softver koji vam pomaže da zaštitite svoju bežičnu mrežu. On automatski uključuje sigurnosne postavke za vaš WLAN i pomaže vam da nadzirete sve korisnike koji su trenutno na vašoj bežičnoj mreži. Posjetite lokaciju www.otosoftware.com.

Zone Labs je lansirao ZoneAlarm Wireless Security. Taj softver automatski otkriva bežične mreže i pomaže vam da ih osigurate. On vam isto tako dopušta da konfigurirate sigurnosne postavke za različite bežične mreže koje obično koristite. Softver obuhvaća vatrozid ZoneAlarm. Detaljne informacije potražite na lokaciji www.zonelabs.com.

LucidLink Wireless Security nudi besplatan softver koji vam pomaže u postavljanju bežičnog kućnog ureda. Proizvod pojednostavljuje korake koji su potrebni za postavljanje i konfiguriranje bežične pristupne točke i za uklanjanje i dodavanje korisnika na WLAN. Softver je besplatan za najviše tri korisnika; on, međutim, zahtijeva da imate jedno odvojeno računalo za žičanoj mreži koje će djelovati kao konzola za upravljanje sigurnošću. To ožičeno računalo ovlašćuje bežična računala da se spajaju na bežičnu mrežu. Detaljne informacije potražite na lokaciji www.lucidlink.com.

9.3 Sigurnost na javnim mjestima

Bežične mreže nisu samo za dom. Mnoga javna mjesta, uključujući kafiće, restorane s brzom hranom, hotele, trgove u gradovima i knjižare te knjižnice nude bežične mrežne veze. Ti javni WLAN-ovi nazivaju se vruće točke *(hotspots)*, i odražavaju nevjerojatnu praktičnost i potražnju za bežičnim povezivanjem. Evo, sada i proizvođač zrakoplova, Boeing, izrađuje zrakoplov koji je opremljen bežičnim pristupnim točkama. Te će pristupne točke voditi podatke do satelitskog tanjura na zrakoplovu, koji će ih potom odašiljati na skupinu satelita i dolje do bazne stanice na Zemlji. Rezultat? Putnici na odgovarajuće opremljenim zrakoplovima moći će se spajati na Internet na visini od 35.000 stopa pomoću standardnih Wi-Fi-omogućenih prijenosnih računala. (Trenutno je ova usluga dostupna u malom broju zrakoplova i to na određenim letovima, ali se uskoro može pojaviti i u zrakoplovima koje vi koristite.)

Postoje dva načina za pronalaženje vrućih točaka. Prvi je da se na vašem ekranu pojavi prozor kada vaša bežična mrežna kartica ili čip otkrije bežičnu mrežu. Drugi

je da korištenjem jedne od nekoliko usluga otkrijete vruće točke diljem zemlje. Intel nudi mehanizme za pronalaženje i američkih i međunarodnih vrućih točaka na adresi http://intel.jiwire.com. Ako volite surfati dok pijete kavu, u SAD-u možete potražiti Starbucks vruće točke na stranici www.starbucks.com/retail/wireless.asp. Još jedna dobra opcija je www.wifinder.com, globalni imenik s 802.11b i 802.11g vrućim točkama.

Neke vruće točke naplaćuju pristup, te se morate pretplatiti na uslugu. Na primjer T-Mobile HotSpot usluga naplaćuje 29,99 USD mjesečno za neograničeni bežični pristup na participirajućim lokacijama koje obuhvaćaju Starbucks, Borders i Kinkos. Da bi vam pomogla osigurati vezu, usluga T-Mobile koristi 802.1x, sigurnosni standard dobrih ljudi iz IEEE-a. Zapamtite da 802.1x nije standard za šifriranje. Ako vidite da neka bežična mreža koristi 802.1x, to znači da ona pruža neke mjere provjere valjanosti. Za šifriranje prometa trebali biste koristiti i WPA ili SSL. (SSL je kratica od Secure Socket Layer. To je protokol koji omogućuje šifrirani prijenos informacija Webom.) Usluga T-Mobile koristi SSL.

Operativni sustav Windows XP ima ugrađenu podršku za 802.1x koja bi prema osnovnoj postavci trebala biti uključena. Da biste saznali kako dvostruko provjeriti je li 802.1x uključeno na vašem računalu otiđite na lokaciju www.microsoft.com i upišite Set up 802.1x authentication u polje za pretraživanje. Pretraživanje će vratiti nekoliko veza do uputa za uključivanje 802.1x.

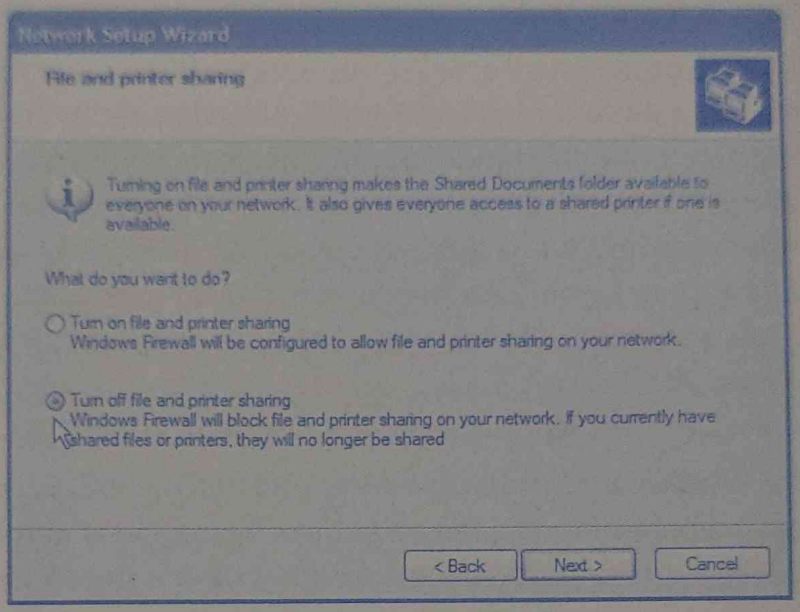
Neosigurane vruće točke

Najveća opasnost s kojom se susreću Wi-Fi korisnici dolazi od vrućih točaka koje se ne zamaraju uključivanjem bilo kakvih mogućnosti šifriranja u bežične pristupne točke. Te neosigurane vruće točke često su besplatne za svakoga tko se želi priključiti. Sigurnosne su mogućnosti isključene da bi korisnici lakše ostvarili pristup. No, to također znači da oni koji njuškaju mogu nanjušiti vaš promet i pokupiti osjetljive informacije.

Ako koristite javne vruće točke, trebali biste poduzeti korake za osiguravanje veze. Zapamtite da računala djeluju kao radio kada koristite bežičnu mrežnu vezu: svi podaci koje generirate emitiraju se svakome unutar dometa.

Neki od ovih koraka su mudri opći sigurnosni postupci, poput provjere funkcioniranja vatrozida i antivirusnog softvera (detaljne informacije o tom softveru nalaze se u 3. i 4. poglavlju). Isto biste tako trebali isključiti dijeljenje datoteka da biste njuškalima zapriječili dobivanje pristupa vašim dokumentima putem Interneta. Windows XP Service Pack 2 ima isključeno dijeljenje datoteka i pisača prema osnovnoj postavci. Ovo možete dvostruko provjeriti klikom gumba Start, odabirom Control Panel pa Network and Internet Connections. Zatim kliknite

Network Setup Wizard (pogledajte sliku 9.1). Morat ćete kliknuti na nekoliko pitanja dok ne dobijete ekran koji vas pita o omogućavanju dijeljenja datoteka i pisača, koji je prikazan na slici 9.4. Ako je dijeljenje datoteka i pisača omogućeno, jednostavno poništite taj potvrdni okvir.



Slika 9.4 Isključivanje dijeljenja datoteka i pisača

Nema li vruća točka omogućene sigurnosne postavke WEP ili WPA, vi ipak možete zaštiti svoj promet s virtualnom privatnom mrežom *(Virtual Private Network* – VPN). VPN-ovi šifriraju promet između dvije točke kao što su vatrozidovi na različitim lokacijama ogranaka korporativne mreže ili između prijenosnog računala i korporativne mreže. VPN-ovi su kreirani da bi štitili korporativni promet koji putuje duž javnog Interneta od ožičenih snifera; oni se danas intenzivno koriste. Šifriranjem svoje bežične veze štitite se od napadača s bežičnim sniferskim alatima.

Ako koristite prijenosno računalo koje ste dobili od korporacije s prije instaliranim VPN klijentom, možete ga upotrijebiti da osigurate svoju bežičnu vezu na neosiguranoj javnoj vrućoj točki. Ako nemate VPN klijent koji vam je dala korporacija, možete se pretplatiti za HotSpotVPN (www.hotspotVPN.com), uslugu iz tvrtke Wi-Fi Consulting čija je početna preplata 10,88 američkih dolara mjesečno. Možete dobiti i jedno-, dvo- ili trodnevnu pretplatu već za 3,88 dolara.

Zli blizanac

Još jedna opasnost na vrućim točkama je napad zlog blizanca *(evil twin attack)*. U osnovi se radi o sljedećem: napadač postavlja prijenosno računalo u blizini javne vruće točke. Potom to prijenosno računalo pretvara u bežičnu pristupnu točku i daje joj isto ime mreže (isti SSID) koje ima legitimna pristupna točka. Ako je signal podvaljene pristupne točke dovoljno jak (ili ako napadač onemogući legitimnu pristupnu točku), zli blizanac se drugim korisnicima predstavlja kao vruća točka. On im čak može prikazati ekran za prijavu koji traži broj kreditne kartice. Ako se potom korisnik prijavi na tu lažnu pristupnu točku, napad može ukrasti sve povjerljive informacije koje korisnik otkriva na Internetu.

Postoji nekoliko dobrih obrana od napada zlog blizanca. Prva je da svoj bežični softver konfigurirate tako da se ne spaja automatski na najbližu mrežu. Još je bolje rješenje aktivirati sigurnosne značajke ugrađene u Wi-Fi tehnologiju (uz pretpostavku da vruća točka ima omogućene sigurnosne postavke). Možete i iskoristiti VPN, što smo upravo opisali.

Imajte na umu da se pljusak napada zlog blizanca tek treba pojaviti, ali je važno da ste svjesni potencijalnih opasnosti te da unaprijed poduzmete odgovarajuće mjere zaštite.

Nemojte provoditi osjetljive transakcije na vrućoj točki

Najsigurnije bi bilo da izbjegavate provođenje *online* bankarstva i e-trgovine dok ste na javnoj vrućoj točki. To bi trebalo ograničiti potencijalnu štetu ako postanete žrtvom napada zlog blizanca ili nekog drugog napada u kojem se putem radiovalova pokušavaju oteti vaše tajne informacije.

9.4 Sigurnost mobilnih telefona i osobnih digitalnih pomoćnika

Mobilni telefoni, osobni digitalni pomoćnici – PDA-ovi *(Personal Digital Assistants)*, i uređaji za bežičnu e-poštu praktični su alati za komunikaciju i produktivnost, koji se brzo približavaju s raznim skupinama značajki i mogućnosti. Možete kupiti PDA koji obuhvaća mobilni telefon i mogućnost slanja i primanja e-pošte, a možete kupiti i mobilni telefon sa značajkama poput pretraživanja Weba, pristupa e-pošti, kalendara, digitalne kamere i izmjene tekstualnih poruka (takvi svestrani mobilni telefoni često se nazivaju smart telefonima). Mobilni telefoni i PDA-ovi mogu koristiti Wi-Fi ili Bluetooth za spajanje na druge mobilne uređaje kao što su obična računala i bežične mreže.

Kako se ovi alati sve dublje ukopavaju u način na koji radimo i kupujemo, oni također mogu postati metama kriminalaca. Obijesni napadači mogu lansirati napade koji smetaju usluzi ili prazne baterije uređaja. Mobilni telefoni i PDA-ovi mogu postati i mete *phishing* napada i drugih *scamova* kojima je cilj žrtvama ukrasti novac.

Trenutno, mobilni uređaji ostali su relativno slobodni od *malware* u usporedbi s osobnim računalima. No, oni se počinju sjedinjavati oko nekoliko uobičajenih operativnih sustava i komunikacijskih vektora, što će *malwareu* olakšati širenje. Zapravo, nekoliko se virusa mobilnih telefona i PDA-ova pojavilo 'u divljini'. Do sada su to uglavnom bili virusi "proof-of-concept" (dokaz koncepta) s ograničenim širenjem i bez zlonamjernog *payloada*.

Sad ćemo pogledati osnove mobilnog operativnog okruženja i komunikacijske vektore koje bi *malware* mogao koristiti za širenje.

Prijenosni operativni sustavi i Bluetooth

Prijenosni se uređaji zasnivaju na dva operativna sustava: PalmOS-u i Microsoft Windows Mobileu (nekadašnjem Pocket PC-u). Mobilni se telefoni sjedinjuju u Symbian operativnom sustavu (OS), što je konzorcij proizvođača telefona. Symbian je razvijen dijelom da spriječi prevlast Microsofta u svijetu mobilne telefonije. Kao što smo raspravili u 4. poglavlju, *malware* se lako širi ako se mali broj operativnih sustava koristi na velikom broju uređaja. To je neizbježna posljedica standardizacije i zahtijeva kompatibilnosti.

Trebali biste znati i za Bluetooth. Bluetooth je bežična tehnologija kratkog dometa (oko 10 metara) koja dopušta da se pojedinačni uređaji spajaju s osobnih mreža (Personal Area Network – PAN). Mobilni telefoni, PDA-ovi i prijenosna računala mogu koristiti Bluetooth za međusobno povezivanje zbog prijenosa digitalnih informacija, uključujući datoteke. Bluetooth koriste miševi, tipkovnice i slušalice. Uz to neki proizvođači dodaju Bluetooth tehnologiju u automobile da bi omogućili hands-free upotrebu telefona.

Bluetooth tehnologiju nadgleda Bluetooth Special Interest Group (SIG). Bluetooth SIG su utemeljile poznate tehnološke kompanije kao što su Nokia, Intel i IBM. Nju trenutno čine i tisuće pridruženih tvrtki članica. Iako Bluetooth nudi praktičnosti za povezivanje različitih proizvoda, vjerojatno je da će postati popularan put širenja infekcije za mobilni *malware*.

Malware mobilnih telefona

Pojavilo se nekoliko vrsta *malwarea* koji ciljaju takozvane smart mobitele. Pregledat ćemo četiri primjera i potom objasniti metode zaštite od tog i drugog *malwarea* smart mobitela:

- Crv Cabir pojavio se u lipnju 2004. godine. On je ciljao operativni sustav Symbian mobilnih telefona i koristio Bluetooth za širenje na druge uređaje. Crv je tražio korisnike da odobre prijem neke poruke. Ako je korisnik prihvatio poruku, od njega se tražilo da instalira datoteku. Oni koji su je instalirali bili su zaraženi crvom. Iako crv nije imao destruktivni kod (*payload*), zaraženi telefoni imali su smanjeni rok trajanja baterije jer je crv stalno tražio druge Bluetooth-omogućene uređaje.
- Trojanski konj pojavio se u studenom 2004.godine i također ciljao Symbian OS. Da bi se inficirali tim trojanskim konjem, korisnici su trebali preuzeti program koji se maskirao kao softverski applet za upravljanje temama na Nokia 7610 smart mobitelu. Ako je korisnik preuzeo taj program, pod imenom Extended Theme.SIS (SIS je kratica za Symbian Installation System), sve su ikone aplikacija bile zamijenjene slikom lubanje s prekriženim kostima (poput one koja označava otrov). Korisnici zaraženi tim trojanskim konjem mogli su i dalje pozivati i primati pozive, ali druge su aplikacije bile onemogućene. Neke varijante ovog trojanskog konja dodale su crvu Cabir destruktivni kod (*payload*).
- U siječnju 2005. godine stručnjaci za istraživanje virusa otkrili su crva Lasco A koji je ciljao Symbian OS preko Bluetootha i korisnike koji su dijelili zaražene SIS datoteke. Korisnici su trebali pristati da se instalira datoteka koja je sadržavala crva. Izvorni kod crva Lasco vrlo je sličan onome crva Cabir.
- Crv Mabir isto cilja Symbian OS i može za širenje koristiti Bluetooth. No, ono po čemu se ovaj crv razlikuje je to da on može slati zaražene datoteke preko MMS-a. MMS, što je kratica od Multimedia Message Service (usluga za multimedijalne poruke), koristi se za slanje digitalnog medija kao što su fotografije i audio datoteke. Zaraženi uređaji počinju tražiti druge mete unutar dometa preko Bluetootha.

Mobilni telefoni nisu još doživjeli glavni napad – *malware* koji ovdje opisujemo ima vrlo nisku stopu zaraze. Jasno je da postoji "know-how" za pisanje virusa za mobilne telefone. Da bi se dogodila značajna provala, piscima *malwarea* preostalo je da otkriju pravu kombinaciju softvera i društvenog inženjeringa. Zato, kao što mudra osoba krpa rupu na krovu po sunčanom vremenu umjesto

da pričeka kišu, korisnici smart mobitela trebali bi poduzeti korake da se zaštite prije nego što neki srečkovič između pisaca virusa objavi vrlo zarazni program.

Kao što je prikazano u tablici 9.2, nekoliko dobro poznatih antivirusnih tvrtki izdalo je antivirusni program za mobilne telefone. (Symantec Mobile Security 4.0 uključuje i vatrozid.) Antivirusni softver štiti vas od poznatih virusa. Ako vaš mobilni telefon ima Web pretraživač, tada možete izravno na telefon preuzeti antivirusni softver. Inače ga možete preuzeti na računalo i prenijeti ga preko kabela ili Bluetooth veze na telefon. Sredinom 2005. godine cijene su se kretale u raspon u od 15,95 do 44,95 američkih dolara.

Osiguravanje Bluetootha

Kao što možete zaključiti prema ovdje opisanom *malwareu*, Bluetooth tehnologija vjerojatno će postati ulazni smjer za *malware* smart telefona. Bluetooth-omogućeni

Tablica 9.2

Antivirusni softver za PDA-ove i mobilne telefone

Proizvod	Proizvođač	Platforma	Operativni sustav	Web lokacija
F-Secure Anti-Virus for Pocket PC	F-Secure	PDA-ovi	Windows Mobile, Windows Pocket PC	www.f-secure.com
F-Secure Mobile Anti-Virus	F-Secure	različiti Nokia mobilni telefoni, N-Gage, SiemensSX1	Symbian OS	www.f-secure.com
Kaspersky AntiVirus Personal	Kaspersky Lab	PDA-ovi	PalmOS, Windows Pocket PC	www.kaspersky.com
PC-cillin for Wireless	Trend Micro	PDA-ovi	PalmOS, Windows Pocket PC	www.trendmicro.com
Symantec AntiVirus for Handhelds	Symantec	PDA-ovi	PalmOS, Windows Mobile, Pocket PC	www.symantec.com
Symantec Mobile Security 4.0	Symantec	Smart telefoni	Symbian OS	www.symantec.com
Trend Micro Mobile Security	Trend Micro	Smart telefoni	Windows Mobile for Pocket PC Phone edition, Windows Mobile for Smartphones, Symbian OS	www.trendmicro.com

uređaji dopuštaju vam da odaberete više ili niže razine sigurnosnih postavki, ali ćete za konfiguriranje trebati proučiti svoj priručnik.

Ako ne koristite Bluetooth, najjednostavniji način i najsigurnija opcija je da ga onemogućite.

Koristite li Bluetooth, možete vidljivost mobilnog telefona postaviti na Hidden ili na mod nemogućnosti otkrivanja. To će spriječiti svaki zaraženi uređaj unutar dometa da vam pošalje *malware*. Pogledajte priručnik svojeg Bluetooth-omogućenog uređaja da biste otkrili kako ga postaviti na Hidden.

Bluetooth vam omogućuje da kreirate parove između Bluetooth uređaja kao što su mobilni telefon i slušalice. Postojano sigurnosno uparivanje šifrira svaku komunikaciju između dva uređaja. No, kod uparivanja neprovjerenih uređaja trebate biti oprezni. Ako postavite uparivanje, upotrijebite postavku Unauthorized; to osigurava da ćete dobiti autorizaciju svakog zahtjeva za uspostavljanjem veze.

Konačno, ako imate omogućen Bluetooth, oprezno postupajte kada prihvaćate neprovjerene datoteke ili aplikacije. Primite li datoteku koju niste očekivali, najsigurnije bi bilo da je odbijete ili izbrišete.

Sigurnost PDA uređaja

PDA-ovi postaju vrlo popularne mete kradljivcima, jer oni često sadrže osjetljive informacije kao što su imena i telefonski brojevi, PIN-ovi, brojevi računa i matični brojevi. PDA-ovi koji koriste Bluetooth suočavaju se s istim ranjivostima kao i Smart telefoni, uključujući i širenje *malwarea*. Kao što je prikazano u tablici 9.2, nekoliko tvrtki nudi antivirusni softver za dlanovnike jer neki virusi koji pogađaju smart telefone inficiraju i PDA-ove.

Do sada je vrlo malo *malwarea* napalo PDA-ove. U kolovozu 2004. godine istraživači su otkrili trojanskog konja Brador, koji je napadao operativni sustav Windows Mobile 2003/Pocket PC. Dok su ljudi koji se bave istraživanjem kreirali PDA *malware* "dokaznog koncepta" u laboratoriju, Brador je bio prvi primjer PDA *malwarea* koji je pronađen 'u divljini'. Kada se uspješno instalirao, trojanski je konj omogućio udaljenom napadaču da kopira datoteke na i s PDA uređaja. Iako je Brador imao vrlo nisku stopu širenja, on je pokazao da pisci *malwarea* imaju sposobnost i sklonost da pogađaju Microsoft-temeljene dlanovnike.

No, najveća opasnost s kojom se suočavaju korisnici PDA uređaja je psihička, a ne tehnološka. Iako se PDA uređaji lako gube i kradu, mnogi se korisnici ne zamaraju time da lozinkom zaštite pristup osjetljivim informacijama. Zato će lopov, koji je stavio ruku na vaš PDA uređaj, imati pristup svim vašim osobnim informacijama koje ste pohranili na uređaj. Svakako upotrijebite lozinku da biste

zaštitili svoje podatke. Neka se lozinka sastoji od kombinacije brojki i slova; to će otežati njezino probijanje. Trebali biste isto tako pohranjivati što je moguće manje osjetljivih informacija na uređaj. Ako baš trebate imati takve informacije na uređaju, razmislite o korištenju softvera za šifriranje koji je dostupan za PDA uređaje i koji se može koristiti kao dodatni sloj za zaštitu podataka.

9.5 VoIP sigurnost

Voice over Internet Protocol (VoIP) je nova tehnologija za ostvarivanje telefonskih poziva preko Interneta. Tradicionalni telefonski pozivi uspostavljali su poseban krug između dva telefona, a glasovi su se prenosili kao digitalni signali preko tog kruga. Nasuprot tome, VoIP ne zahtijeva poseban krug između dva pozivatelja. On uzima glas govornika i "lomi" ga u pojedinačne pakete koji se usmjeravaju preko javnog Interneta na isti način na koji se odvija promet e-pošte i Weba. (Detalji o radu IP-a nalaze se u 3. poglavlju.)

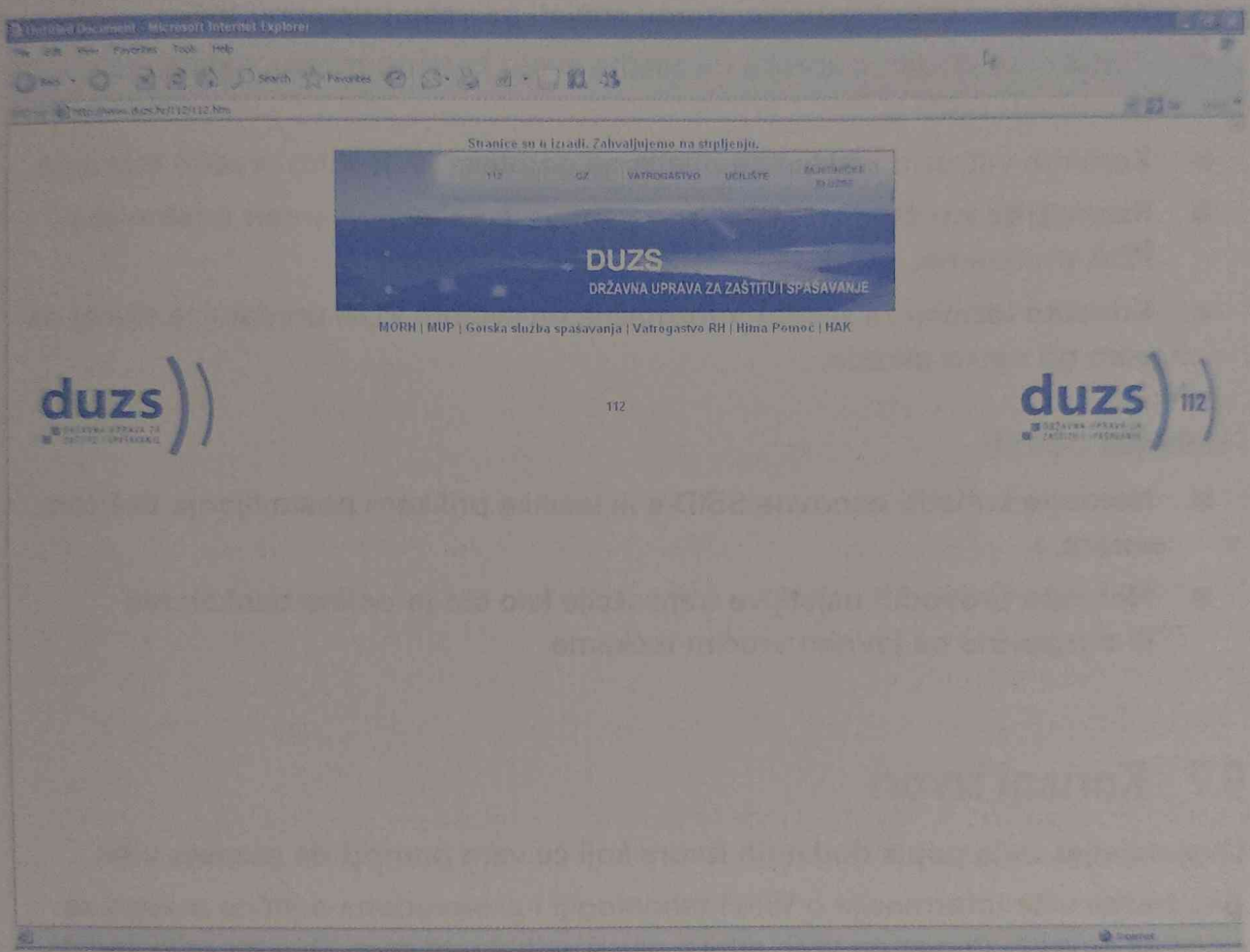
Neke kompanije kao što su Vonage, Packet8, Verizon i SBC nude korisnička VoIP rješenja koja stoje manje od standardne telefonske usluge. Za te VoIP usluge trebate kupiti poseban adapter u koji ćete uključiti svoj telefon i svoju širokopojasnu (odnosno kabelsku ili DSL) Internet vezu.

Druga opcija je softver Skype (www.skype.com), koji vam omogućuje da besplatno telefonirate sa svojeg računala s drugim Skype korisnicima. Skype radi pod sustavima Windows, Macintosh i Linux. Sve što vam je potrebno jesu slušalice s mikrofonom koje možete priključiti na svoje računalo i Internet vezu. Do sada je preuzeto 108 milijuna kopija softvera Skype. Skype nudi i uslugu koja se plaća i zove se SkypeOut; ona vam omogućuje da sa svojeg računala pozivate obične telefone.

Iako VoIP predstavlja jeftiniji način telefoniranja, on ima i nekoliko potencijalnih sigurnosnih problema. Prvi je taj da ćete morati otvoriti široki raspon izlaznih portova i nešto manji raspon ulaznih portova u svojem vatrozidu. Napadači ili automatizirani *malware* mogli bi pokušati iskoristi te otvorene portove za dobivanje pristupa vašem računalu. Trenutno nije bilo nikakvih izvještaja o obuhvatnijim pokušajima zlorabljenja otvorenih portova VoIP-a, ali što će se više ljudi pretplaćivati na ovakve usluge, ti će pokušaji vrlo vjerojatno porasti. Isto tako, budući da se VoIP oslanja na vašu Internet vezu, svaki napad na tu vezu može "odrezati" vašu VoIP telefonsku uslugu. Uz to, ako vaš ISP pretrpi razne gubitke (na primjer gubitak snage ili možda gubitak usluge uzrokovan DoS napadom), to će utjecati na vašu VoIP telefonsku uslugu.

VoIP i 112

Imamo i mi svoj 911 za hitne pozive! To je broj 112 koji vrijedi u cijeloj Europi. No, VoIP pozivi broja 112 kod nas nisu uzeli maha kao što su u SAD-u pozivi broja 911, tako da je pozivanje ovog broja korištenjem VoIP-a još u povojima. Za sada vam jedino mogu predložiti da pratite novosti o opcijama službe 112 koja pripada pod Državnu upravu za zaštitu i spašavanje na adresi www.duzs.hr ili posebno na stranici za službu 112 http://www.duzs.hr/112/112.htm, koja sada izgleda kao što je prikazano na slici 9.5.



Slika 9.5 Web stranica službe 112

9.6 Popis za provjeru

Upotrijebite ovaj popis za provjeru kao brzi referentni vodič kroz gradivo izneseno u ovom poglavlju.

Učinite

- Zapamtite da radio signale koje emitira bežična mreža može uloviti druga bežična računalna oprema.
- Uključite WEP ili WPA za šifriranje vašeg bežičnog prometa i osigurati da se samo ovlašteni korisnici mogu spajati na vašu pristupnu točku.
- Poduzmite dodatne korake da zaštite svoju bežičnu mrežu, uključujući promjenu SSID-a.
- Koristite vatrozid i isključite dijeljenje datoteka na javnim vrućim točkama.
- Razmotrite korištenje antivirusnog softvera na svojim smart telefonima i PDA uređajima.
- Koristite lozinku za zaštitu informacija na svojem PDA uređaju za slučaj da vam ga netko ukrade.

Nemojte učiniti

- Nemojte koristiti osnovne SSID-e ili lozinke prilikom postavljanja bežične mreže.
- Nemojte provoditi osjetljive transakcije kao što je *online* bankarstvo ili e-trgovina na javnim vrućim točkama.

9.7 Korisni izvori

Ovaj odjeljak daje popis dodatnih izvora koji će vam pomoći da saznate više.

Ako tražite više informacija o Wi-Fi tehnologiji i proizvodima odlično mjesto za početak je Wi-Fi Planet na Web adresi www.wi-fiplanet.com. Ova lokacija sadrži priručnike, recenzije proizvoda i sigurnosne informacije i još mnogo toga.

Korisne ćete informacije o standardima 802.11b, g i bežičnim standardima naći na stranici www.linksys.com, odabirom Learning Center pri vrhu polazne stranice, a zatim Network Security.

Microsoft nudi informacije o bežičnim mrežama i sigurnosti te pruža savjete o sigurnosti na javnim vrućim točkama. Posjetite stranicu www.microsoft.com/atwork/stayconnected/hotspots.mspx.

Intel nudi savjete za bežičnu sigurnost na adresi www.intel.com/personal/do_more/wireless/security/.

Detaljne informacije o Bluetooth nudi Wikipedia, *online* enciklopedija. Pođite na lokaciju www.wikipedia.org pa u polje za pretraživanje upišite Bluetooth.

10. poglavlje

Privatnost i Internet

Živimo u vrijeme sumanutog skupljanja i analiziranja podataka. Elektroničke mreže su toliko ojačale u trgovanju i komunikacijama da omogućuju do sada neviđeno skupljanje, pohranjivanje i dijeljenje (ili prodavanje) osobnih informacija. Ovaj žrvanj pokreću dvije sile, jedna komercijalna i druga vladina. Svaka sila ima vlastite motive i svaka svoje vlastite resurse (iako se u mnogim slučajevima ti resursi približavaju), ali se obje "napajaju" iz zajedničkog izvora: mene i vas.

U komercijalnoj areni, mešetari podataka gomilaju baze podataka sa značajnim činjenicama kao što su vaš matični broj, datum rođenja, bračni status i mjesečne rate kredita kao i naoko bezvrijedne informacije kao što je vaša omiljena zubna pasta. Ti se podaci skupljaju i njima se trguje ili ih se prodaje raznim stranama. Zauzvrat, te strane analiziraju podatke u nadi da će skupiti osnovne korisne informacije. Je li ova osobina rizična za dobivanje kredita? Ima li čovjek koji se prijavio za posao kriminalistički dosje? Bi li ova osoba mogla biti zainteresirana za informacije o novoj marki zubne paste?

S vladine strane postoji dugačka tradicija prikupljanja obavijesnih podataka, domaćih i međunarodnih, preko sudova i agencija za špijunažu. Ova se obavještajna metoda koristi za stjecanje prednosti u diplomaciji, trgovini, borbi protiv kriminala, ratova i nacionalne sigurnosti. Prije pedeset godina značajni su se vladini resursi slijevali u infrastrukturu za skupljanje informacija u doba Hladnog

rata. U sadašnje vrijeme glavni je pokretač raširenog skupljanja podataka borba protiv terorizma.

Većina građana ima koristi od te žetve informacija koju provodi vlada i komercijalni sektor. Mešetari podataka nam olakšavaju da dobivamo kredite, kupujemo kuće ili iznajmljujemo stanove te da smo obaviješteni o čudnim aktivnostima na našim kreditnim karticama itd. Oni nam također omogućuju da koristimo prednost komercijalne konkurencije (kao što je dobivanje kupona za različite marke zubnih pasta) korporativne suradnje (kao što je dobivanje zrakoplovnih milja za kupnju zrakoplovnih karata kreditnim karticama). U međuvremenu lokalne državne i federalne agencije mogu pratiti i dijeliti informacije za hvatanje kriminalaca i borbu protiv prijevara. Vlada se također nada da bi informacije koje skupljaju zakonodavna tijela i antiterorističke agencije mogle spriječiti ponavljanje 9/11 napada.

No ovo masovno skupljanje informacija ima i svoju tamnu stranu; onu koja radi na teorijama konspiracije zlokobnih korporativnih klika koje diktiraju globalne poslove ili Orwellovske scenarije sveznajućeg, sveprisutnog nadzora države. Problem je u tome što ovi scenariji sadrže zametak istine. U 2. poglavlju "Sprječavanje krađe identiteta" kratko je spomenut skandal ChoicePointa, u kojem je mešetar podataka ChoicePointa objavio da je prodao osjetljive osobne informacije 145 000 ljudi kradljivcima identiteta koji su glumili vlasnike legitimnih tvrtki. Taj je skandal otkrio Amerikancima koliko je mnogo informacija o njima prikupljeno – i koliko se novaca zarađuje na tim informacijama. Advokati za privatnost ukazali su na sustave skupljanja podataka koje sponzorira vlada kao što su Echelon (globalni elektronički sustav nadzora koji dijelom vode National Security Agency – NSA) i Carnivore (program koji omogućuje zakonodavnim agencijama SAD-a da "prosijavaju" e-poštu i drugu komunikaciju na Internetu). Činjenica je da koristi mehanizma za skupljanje podataka imaju svoju cijenu: erozija privatnosti s obzirom na naše navike, preference i osobne informacije i vrlo velika vjerojatnost da bi se te informacije mogle zlorabiti.

Na primjer, kradljivci identiteta rutinski manipuliraju čuvarima podataka da otvaraju lažne račune. Nedužni se građani ne mogu ukrcati u avione jer se njihova imena nalaze na popisu terorista kojima nije dozvoljeno putovanje avionom. (Čak ni moćnici nisu imuni na ovakve pogreške. 2004. godine senator Ted Kennedy, vjerojatno jedan od najprepoznatljivijih političara u SAD-u, zadržan je u zračnoj luci upravo zbog toga.)

Pogrešne informacije mogu imati i političke reperkusije. Za vrijeme predsjedničkih izbora 2000. godine, stotinama je birača zabranjen pristup biralištima u Floridi

jer su pogreškom popisani kao bivši kriminalci koji su izgubili pravo na glasanje. A u ratu protiv terorizma nevine se osobe mogu pritvoriti bez zakonskog naloga.

Na žalost, što se tiče skupljanja podataka, duh je izašao iz svjetiljke. Međutim, možete poduzeti korake da biste zadržali neku dozu privatnosti, barem *online*. Ovo poglavlje ispituje različite načine traženja i ostvarivanja prava za privatnost na Internetu. Pokazat ćemo vam kako otkriti koje podatke o vama skupljaju glavni mešetari podataka.

10.1 Opcije privatnosti na Internetu

Moguće je postići određenu dozu privatnosti kada govorimo o korištenju Interneta. Postoji softver koji može šifrirati e-poštu i instant poruke koje šaljete te datoteke i mape koje spremate na svoje računalo. Uz to, mehanizmi za anonimnost na Webu mogu vam pomoći da zamračite lokacije koje posjećujete.

Šifriranje je proces u kojem se informacije (koje se nazivaju i običan tekst) provlače kroz matematički algoritam da bi se proizveo nečitki tekst. Jedini način za pretvaranje nečitkog u čitki tekst je nekim ključem. Ključ je poput tajnog koda koji se kombinira s drugim matematičkim operacijama da se nečitki tekst pretvori natrag u običan tekst. Kao što smo već nekoliko puta raspravljali u drugim poglavljima, Internet se oslanjanja na šifriranje kod e-trgovine i provjere valjanosti uključenih osoba koje možda nemaju mehanizme za izgradnju povjerenja ili razmjenu identifikacijskih akreditiva u stvarnom svijetu.

Osnove šifriranja

Općenito govoreći, postoje dvije vrste digitalnog šifriranja: simetrično i asimetrično. Kod simetričnog šifriranja isti se ključ koristi za šifriranje običnog teksta i dešifriranje nečitkog teksta. Sigurnost šifriranja ovisi dijelom o algoritmu koji se koristi i o duljini ključa. Standardni američki algoritam zove se Advanced Encryption Standard (AES). Taj algoritam podržava ključeve raznih duljina. Duljina ključa mjeri se u bitovima. Snaga duljine ključa procjenjuje se po tome koliko bi komercijalno dostupnom računalu trebalo vremena da dešifrira šifriranu poruku isprobavanjem svih mogućih kombinacija brojki i slova. To se naziva napad golom silom (*brute-force*) i najmanje je elegantna metoda provaljivanja šifre. Međutim, radi se o prilično točnom mjerenju, jer trebate pretpostaviti da vaš protivnik ima pristup široko dostupnoj računalnoj tehnologiji.

Danas se 40-bitni ključevi smatraju beskorisnima; 128-bitni, 256-bitni i 512-bitni ključevi su industrijski prihvatljivi; 1024-bitni ključevi smatraju se već nekom vrstom paranoje, a 2048-bitni ključevi su za ljude koji bi vam mogli reći što su šifrirali ali će vas nakon toga ubiti.

Simetrično šifriranje dobro je opremljeno za šifriranje podataka kao što su datoteke, mape i dokumenti. Kod njega je problem u tome što je manje korisno za slanje šifriranih poruka. U poruku ne možete staviti ključ jer bi je svatko tko ju presreće mogao lako dešifrirati. (Kriptografi *uvijek* pretpostavljaju da ih netko uhodi.) Ključ možete staviti na disk i poslati ga običnom poštom, ali tada riskirate da se disk izgubi ili presretne. Mogli biste smisliti i način da potajno dostavite disk, ali ako protivnik nadzire vašu komunikaciju, on će naći gdje ga može pronaći. Pa ako i sredite prijenos diska u tajnosti, što se događa ako primatelj živi na drugom kraju zemlje? Disk biste mu mogli odnijeti, ali u tom slučaju možete jednostavno isporučiti poruku bez gnjavaže sa šifriranjem.

Rješenje ovog problema je asimetrično šifriranje, koje se naziva i šifriranje s javnim ključem. Pri asimetričnom šifriranju jedna matematička funkcija generira dva ključa: jedan se ključ koristi za šifriranje običnog teksta, a drugi za njegovo dešifriranje. Ključ po kojem se šifrira običan tekst ne može se koristiti za dešifriranje tog teksta i obratno. Činjenica da je takva operacija moguća, sama je po sebi prilično impresivna. Iza asimetričnog šifriranja krije se mnogo kompliciranih matematičkih funkcija (što potvrđuje činjenica da su s MIT-a sva tri čovjeka koji su otkrili najpopularniji asimetrični ključ, poznat kao RSA). Za nas je dovoljno da znate da ta dva ključa rješavaju problem koji postoji kod simetričnog šifriranja.

Osnovna je ideja sljedeća: Iva generira par javnog ključa. Jedan ključ drži u tajnosti, a drugi objavljuje u javnom direktoriju na Internetu. Ako Marko želi Ivi poslati šifriranu poruku, jednostavno će potražiti njezin javni ključ u direktoriju i upotrijebiti ga za šifriranje svoje poruke. Kada Iva primi tu poruku, upotrijebit će svoj privatni ključ da je dešifrira. Želi li potom Marku odgovoriti na poruku, potražit će njegov javni ključ i upotrijebiti ga za šifriranje odgovora.

Kao dodatni sloj sigurnosti, umjesto da jednostavno koristi Ivin javni ključ za šifriranje poruke, Marko može upotrijebiti jaki simetrični ključ za šifriranje poruke, a zatim Ivin javni ključ za šifriranje simetričnog ključa. Potom će poslati oba dijela običnog teksta Ivi. Iva koristi svoj privatni ključ za šifriranje simetričnog ključa, a zatim simetrični ključ za dešifriranje poruke.

Digitalni potpisi i digitalni certifikati

OK, sada ste vjerojatno već zbunjeni. Ako niste, tada se stvari ovdje kompliciraju. Šifriranje s javnim ključem omogućuje i korištenje digitalnih potpisa i digitalnih certifikata. Digitalni potpis ima dvije namjene. Prvo, on provjerava dolazi li poruka od osobe koja tvrdi da je poruku poslala. Drugo, on sprječava da s porukom petlja netko treći.

Da bi kreirala digitalni potpis Iva uzima svoju nešifriranu poruku i provlači je kroz algoritam za "sjeckanje" (poznat i kao *hash* algoritam). *Hash* algoritam je matematički proces koji generira komprimiranu poruku. Ono što je problem kod *hash* algoritma je činjenica da ćete, koliko god puta provlačili istu poruku kroz isti algoritam, svaki put dobivati identičnu komprimiranu poruku. No, ako promijenite samo jedno slovo u poruci, i potom je provučete kroz *hash* algoritam, dobit ćete drugačiju komprimiranu poruku. Zato, ako primatelju šaljete poruku i komprimiranu poruku (i *hash* algoritam koji ste upotrijebili), primatelj će na tu poruku moći primijeniti isti *hash* algoritam. Ako se dvije komprimirane poruke podudaraju, primatelj će biti siguran da poruka nije promijenjena.

Zato Iva provlači svoju poruku kroz *hash* algoritam i dobiva komprimiranu verziju poruke. Tu verziju šifrira svojim *privatnim* ključem. Marko zatim koristi Ivin javni ključ za dešifriranje poruke. Uspješno dešifriranje dokazuje Marku da je poruku zaista poslala Iva, jer samo ona ima pristup svojem privatnom ključu. Digitalni potpisi nisu namijenjeni za zaštitu poruka od njuškala, oni dokazuju da je pošiljatelj autentičan i da je poruka potpuna.

Naravno, jedan problem s tehnologijom javnih ključeva je kako provjeriti da je vlasnik javnog ključa osoba koja se predstavlja kao vlasnik. Na primjer, ništa ne može spriječiti Vesnu od objavljivanja svog javnog ključa pod Ivinim imenom. Zato, Marko misli da šalje zaštićenu poruku Ivi, ali je zapravo šalje Vesni. (A vi ste mislili da je agent Mulder paranoičan? On nema veze s kriptografijom.)

Tu sada uskaču digitalni certifikati. Digitalni certifikat sadrži privatni ili poslovni javni ključ. Digitalni certifikati, koje izdaju provjerene treće strane (koje se nazivaju certifikacijski autoriteti, odnosno *Certificate Authority*) djeluju kao oblik elektroničke provjere vjerodostojnosti koja potvrđuje da je vlasnik certifikata onaj za kojeg se predstavlja. Na digitalni certifikat možete gledati kao na vozačku dozvolu. Nju izdaje provjerena ustanova i pruža prihvatljivu potvrdu vašeg identiteta.

Naravno, čak se i vozačke dozvole krivotvore, pa ako se pitate kako možete vjerovati organizaciji koja je izdala digitalni certifikat, tada napokon počinjete učiti razmišljati kao kriptograf. Prije su se izdavali lažni digitalni certifikati i to će se

vjerojatno ponovno dogoditi. Međutim, lanac povjerenja treba negdje imati kraj (ili početak), a nekoliko je tvrtki, uključujući tvrtku VeriSign, kotiraju vrlo dobro kao certifikacijski autoritet i izdavač digitalnih certifikata u Internetskoj zajednici.

Iako ovaj elaborat zvuči toliko kompliciran da djeluje vrlo nepraktično za realan svijet, šifriranje javnim ključem stvarno funkcionira. Cijelokupno e-poslovanje na Internetu temelji se na tehnologiji javnih ključeva; svaki put kada nešto kupite na Amazonu ili provedete *online* bankarsku transakciju, koristite infrastrukturu javnog ključa.

Šifriranje javnim ključem igra važnu ulogu i u popularnom obliku šifriranja e-pošte, o čemu govorimo u sljedećem odjeljku.

Šifriranje e-pošte

Najpopularnija implementacija tehnologije javnog ključa za šifriranje e-pošte zove se PGP. PGP je kratica od Pretty Good Privacy (*prilično dobra privatnost*) čiji je tvorac Phil Zimmermann. To je i naziv korporacije za izradu komercijalnog softvera za šifriranje, uključujući PGP Desktop Home 9.0. Ovaj proizvod možete koristiti za šifriranje odlazne e-pošte, AOL Instant Messenger poruka i nekih datoteka na svojem PC-u. Softver podržavaju Microsoft Outlook i Thunderbird, klijent e-pošte koji je razvila Mozilla Foundation, a koja proizvodi i pretraživač Firefox Web. Dostupan je *online* na adresi www.pgpstore.com.

Možete preuzeti i besplatnu verziju softvera otvorenog izvora pod nazivom Open PGP na adresi www.pgpi.org. Morat ćete kliknuti na nekoliko stranica da biste došli do do Windows XP verzije.

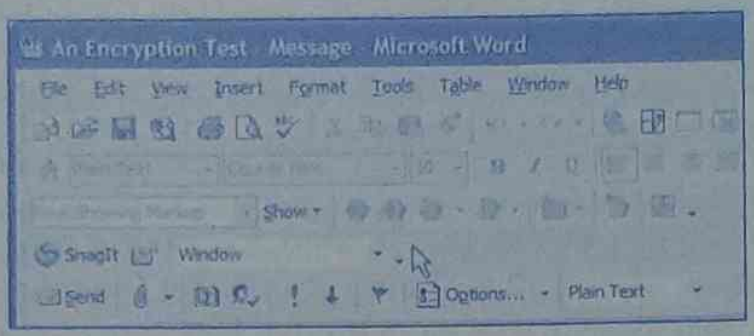
Rješenje za šifriranje e-pošte može vam dati i tvrtka Hushmail. Hushmail koristi Open PGP standard i nudi verziju Web pošte i verziju koja radi s Outlookom, klijentom e-pošte koji je ugrađen u Microsoft Office. Detalje potražite na adresi www.hushmail.com.

Uz softver nezavisnih proizvođača, Outlook, klijent e-pošte koji se isporučuje s Microsoft Officeom, vam omogućuje da šifrirate svoje izlazne poruke e-pošte. On se također temelji na tehnologiji javnog ključa, pa biste trebali preuzeti i kupiti digitalni certifikat. Kada prvi put budete pokušali poslati neku šifriranu poruku Microsoft će vas provesti kroz korake koje je potrebno poduzeti da biste dobili taj digitalni certifikat.

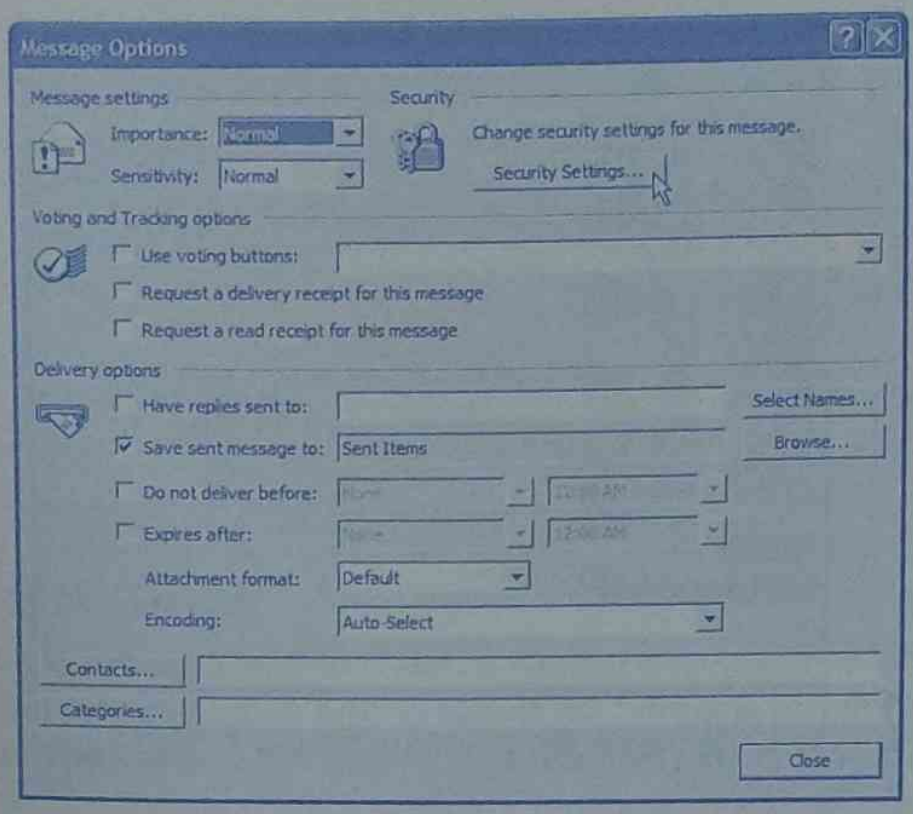
No, prije nego što prođete kroz sve te korake, imajte na umu da možda nećete moći slati šifrirane poruke iz Outlooka ako primatelji poruka nisu kreirali digitalne potpise i registrirali ih na javnom *online* direktoriju. Razlog tome je, ako se sjećate iz rasprave o šifriranju javnim ključem, taj da pošiljatelj treba koristiti

javni ključ primatelja da bi transakcija uspjela. Ako svoje primatelje možete nagovoriti da kupe vlastite digitalne certifikate, kako biste u Outlooku koristili šifriranu e-poštu, trebate poduzeti sljedeće korake.

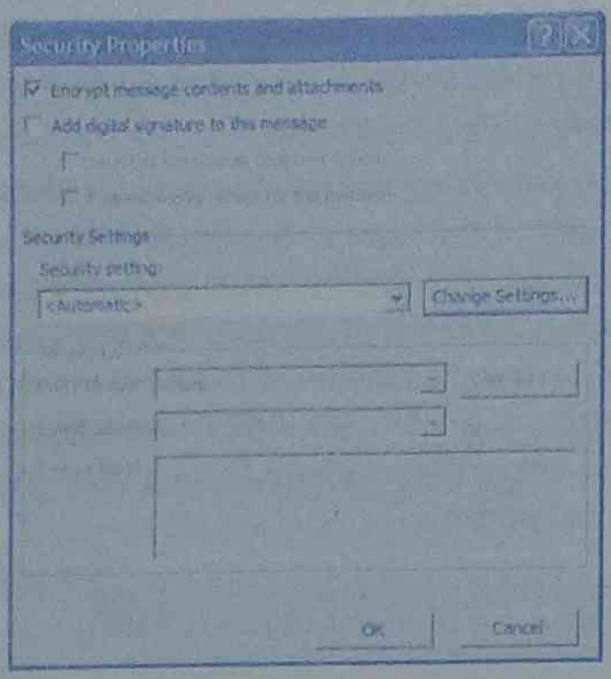
Najprije otvorite Outlook i sastavite poruku. Kada ste gotovi, kliknite gumb Options, kao što je prikazano na slici 10.1. Kada se otvori prozor Message Options, prikazan na slici 10.2, kliknite gumb Security Settings. Otvorit će se prozor, koji je prikazan na slici 10.3. Potvrdite okvir Encrypt message contents and attachments. Za sada nemojte potvrditi okvir Add digital signature to this message, jer najprije morate instalirati digitalni certifikat. Kliknite OK u dijaloškom okviru Security Properties. Sada biste se automatski trebali vratiti na svoju poruku. Odaberite adresu primatelja i pošaljite mu poruku.



Slika 10.1 Klik gumba Options nakon sastavljanja poruke u Outlooku

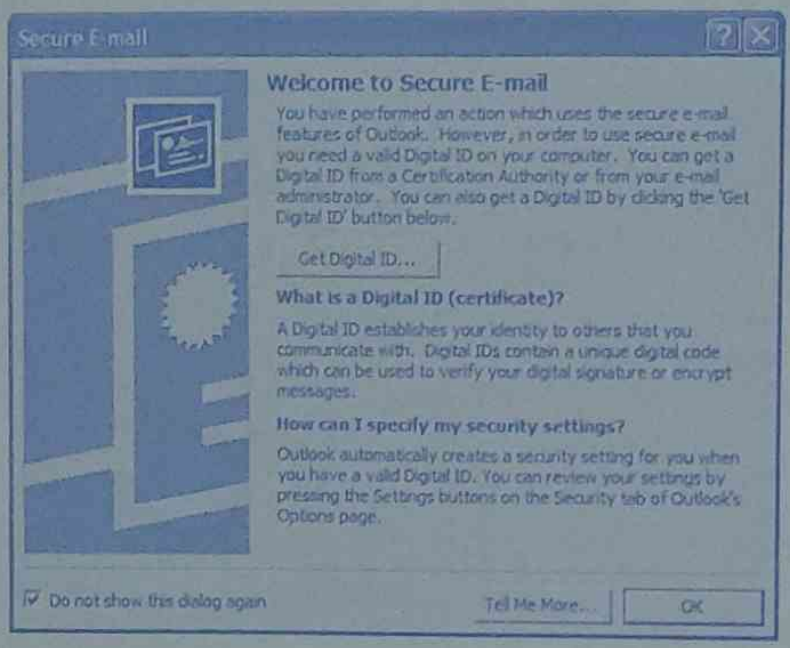


Slika 10.2 Dijaloški okvir Message Options



Slika 10.3 Dijaloški okvir Security Properties

Nakon što ste napisali poruku kliknite gumb Send. Vidjet ćete prozor Welcome to Secure E-mail prikazan na slici 10.4. Kliknite gumb Get Digital ID.... To će vas odvesti na Microsoft Web lokaciju s vezama do dva izdavača digitalnih certifikata: GeoTrusta i VeriSigna.



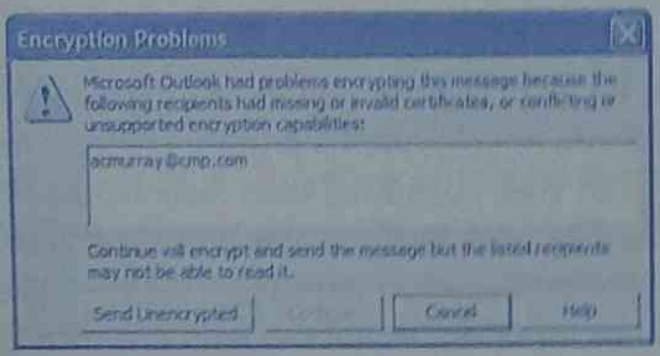
Slika 10.4 Dijaloški okvir Welcome to Secure E-Mail

GeoTrustov Personal Digital ID omogućuje vam da digitalno potpisujete svoje Word dokumente te da digitalno potpisujete i šifrirate e-poštu. To će vas godišnje stajati 19,95 američkih dolara.

VeriSignov Digital ID ima također cijenu od 19,95 američkih dolara godišnje. Tako dobivate 1000 dolara vrijednu zaštitu od ekonomskih gubitaka, ako se vaš digitalni certifikat ošteti, izgubi ili zlouporabi. VeriSign vas postavlja na popis u javni direktorij tako da svatko, tko vam želi poslati šifriranu poruku, može pronaći vaš javni ključ. Moguće je i besplatno pregledavanje drugih digitalnih certifikata koje je izdao VeriSign. VeriSign nudi i besplatnu probnu verziju digitalnog certifikata u trajanju od 60 dana.

Za certifikat se morate registrirati. Za proces registracije trebate pristup svojoj e-pošti (a za GeoTrust i telefonu). Registracija je prilično jednostavna; traži da date svoje ime i adresu e-pošte. Nakon registriranja, kliknite gumb za instaliranje digitalnog certifikata. Pokretanjem instaliranja Microsoft bi mogao prikazati upozorenje Potential Scripting Violation. Kliknite Yes da biste nastavili.

Kada instalirate digitalni certifikat, napokon možete kliknuti gumb Send u Microsoft Outlooku. Međutim, kao što smo spomenuli, može doći do neprilika ako ljudi kojima šaljete šifrirane poruke nemaju digitalne certifikate (pogledajte sliku 10.5). Uz to, neki sustavi za poštu ne podržavaju ili imaju onemogućeno S/MIME (Secure/Multipurpose Internet Mail Extensions, standard šifriranja s javnim ključem), ili možda ne prihvaćaju šifrirane poruke jer antivirusni skeneri ne mogu skenirati šifriranu e-poštu.



Slika 10.5 Dijaloški okvir Encryption Problems

Šifriranje datoteka i mapa

Šifriranje osobnog računala je mudro ako na njemu držite osjetljive informacije kao što su *online* povrati poreza, brojevi računa itd. Šifriranje tih informacija naročito je dobro jer vas ono štiti bude li vaše računalo ukradeno ili ako ga izgubite. (Prema istraživanju iz 2001. godine, u londonskim je taksijima zaboravljeno tisuće prijenosnih računala.)

Većina proizvoda za šifriranje na osobnim računalima ide u istom smjeru. Odabirete datoteku ili mapu koju ćete šifrirati. Da biste je dešifrirali, trebat ćete upisati lozinku. Tako radi ikona Icon Lock-iT XP. Za dodatne informacije posjetite lokaciju www.iconlockit.com. Kao što smo već rekli, PGP Desktop obuhvaća šifriranje e-pošte i datoteka. Programe za šifriranje možete pronaći i *online*. Na primjer, *PC Magazine* ima program za šifriranje pod nazivom File Warden 2. Za besplatno preuzimanje jednostavno otiđite na adresu www.pcmagazine.com i potražite File Warden 2.

Proizvodi za anonimnost na Webu

Proizvodi za anonimnost na Webu mogu vam pomoći da, prilikom korištenja Interneta, zaštitite svoju privatnost. Proizvodi za anonimnost uklanjaju informacije koje bi se mogle upotrijebiti za identificiranje i praćenje vaših navika surfanja po Webu. Oni također usmjeravaju Web promet kroz brojne usmjernike i poslužitelje kako bi zameli trag do ishodišta i odredišta (to se ponekad naziva i *onion routing*; *onion* znači luk, pa se ovdje koristi kao asocijacija zbog svojih slojeva, od kojih svaki štiti onaj ispod sebe, pa ga morate 'ljuštiti' sloj po sloj). Center for Democracy and Technology (Centar za demokraciju i tehnologiju) nudi dugačak popis usluga za anonimnost na Webu, na adresi www.cdt.org/resourcelibrary/Privacy/Tools/Anonymizer/.

Mogli biste provjeriti i program za anonimnost pod nazivom Tor. Tor sponzorira Electronic Frontier Foundation (EFF), potporna grupa za pravo privatnosti. Da biste saznali više, posjetite adresu http://tor.eff.org/.

Još jedna od opcija je Privoxy na adresiwww.privoxy.org. Privoxy je Web *proxy* koji može "skinuti" oglase, banere i iskočne poruke te upravljati kolačićima. *Proxy* je stroj koji posreduje kod Internet veza s drugim računalima. Odnosno, umjesto da idete ravno na neki Web poslužitelj kako biste učitali Web stranicu, idete do proxyja. Proxy odlazi na poslužitelj i za vas preuzima Web stranicu. U međuvremenu, proxy može ukloniti svaki nepoželjni element prema vašem zahtjevu. On također sudjeluje u praćenju kolačića. Web poslužitelj ne može postaviti kolačić na vaše računalo jer ono nikada nije posjetilo tu Web stranicu.

Drugi način da se stekne kakva-takva privatnost na Internetu je uklanjanje kolačića za praćenje s računala. Kolačići za praćenje bilježe Web stranice koje posjećujete i oglase koje klikate, unutar neke tekstualne datoteke pohranjene na vašem računalu. Kolačići za praćenje koriste se i za skupljanje informacija o vašim navikama surfanja zbog isporuke ciljanog oglašavanja i statističkih podataka o Web stranicama koje posjećujete. Sve Web lokacije koje posjećujete postavljaju kolačiće na vaše računalo kako bi pomogle Web pretraživaču da zapamti gdje se

nalazite na lokaciji i kako bi se vama prilagodila Web lokacija "pamćenjem" vaših preferenci i postavki. No, kolačići za praćenje dijele informacije s trećim stranama. Ti kolačići neće naštetiti vašem računalu, ali predstavljaju provalu u vašu privatnost. Kolačiće za praćenje možete otkriti, ukloniti ili blokirati pomoću *anti-spyware* softvera (pogledajte 5. poglavlje, "Kako se riješiti nepoželjnih gostiju?, 2. dio: *spyware*, *adware* i trojanski konji").

10.2 Kako postupati s mešetarima podataka

Mešetari podataka kao što su ChoicePoint, LexisNexis i Acxiom o nama skupljaju nevjerojatne količine podataka. Te tvrtke samostalno skupljaju podatke iz javnih izvora, kao što su telefonski imenici i zapisi o javnim prodajama kuća i stanova, što su sve javni podaci. Ali oni isto tako uzimaju podatke od trećih strana. Na primjer, Acxiom većinu svojih informacija dobiva od tvrtki koje žele sabrati te podatke kako bi doznale više o svojim klijentima. Prema autoru Robertu Harrowu, Jr., i njegovoj knjizi *No Place to Hide* (Nemamo se kamo sakriti), sve tvrtke kao što su Sears, Hallmark Cards, Safeway i Lands End šalju informacije koje su skupile o svojim klijentima Acxiomu. Povrh toga, banke i kompanije za izdavanje kreditnih kartica šalju svoje podatke u Acxiomove baze podataka.

Za korisnike koji mogu poduzimati mjere da bi ograničili podatke koje pružaju pojedinim tvrtkama i vladinim agencijama problem je u tome što ti isti entiteti mogu sve te različite informacije o vama učitati u masivan računalni sustav koji povezuje i analizira goleme količine informacija.

Jedan od načina na koji možete izbjeći da netko ima dosje o vama, je da što je moguće više informacija o sebi držite podalje od javnog bilježenja. Chris Hoofnagle, direktor Electronic Privacy Information Centera (EPIC) na Zapadnoj obali, organizacije za potporu privatnosti, nudi tri savjeta:

- Ako kupujete ili prodajete kuću ili stan, osigurajte da se u javnom zapisu ne pojave vaš matični broj i datum rođenja.
- Kada se pretplaćujete na telefonsku i druge javne usluge, inzistirajte na tome da odnosna tvrtka ne koristi vaš matični broj ili broj osobne iskaznice. Idete li ovim putem, možda ćete trebati ostaviti neki novčani polog.
- Nemojte da vas zatvore, jer su takvi zapisi javni.

Možete također poduzeti korake da biste ograničili ono što mešetari podataka rade s informacijama, a u nekim slučajevima možete dobiti pristup informacijama koje o vama čuvaju pa odlučiti da vas se isključi iz baza podataka.

Acxiom (www.acxiom.com)

Acxiom ima dva skupa proizvoda: InfoBase Marketing i InfoBase te Sentricx Reference. Acxiomovi klijenti koriste InfoBase Marketing za kreiranje popisa za ciljano oglašavanje. InfoBase Marketing ne obuhvaća informacije o kreditnim karticama, zdravstvenom stanju ni matične brojeve. Iz baze podataka InfoBase Marketinga možete se povući, što znači da tvrtke kojima ste zanimljivi ne mogu pristupati vašim informacijama preko Acxioma, pa nećete dobivati promotivne telefonske pozive, direktnu poštu (tzv. *junk* poštu), kataloge ili e-poštu tvrtki koje posluju s Acxiomom. Formular za povlačenje možete zatražiti e-poštom na adresu optoutUS@acxiom.com.

Acxiomove InfoBase i Sentricx Reference usluge uključuju financijske informacije i matične brojeve. Acxiomovi klijenti koriste te usluge za radnje poput provjeravanja zaposlenika i odobravanja hipotekarnih kredita. Agencije za provođenje zakona mogu također dobiti pristup informacijama iz InfoBasea i Sentricx Referencea. Informacijama koje su o vama pohranjene možete pristupiti tako da zatražite Reference Information Report. Za to Acxiom naplaćuje 5 dolara naknade. Izvještaj možete zatražiti i slanjem poruke e-pošte na adresu referencereport@acxiom.com.

Za detaljne informacije otiđite na lokaciju www.acxiom.com i kliknite vezu Privacy na lijevom dijelu polazne stranice. Da biste dobili više informacija o pristupu informacijama koje Acxiom prikuplja o vama možete u polje za pretraživanje na polaznoj stranici upisati Notice, Access, Choice.

ChoicePoint (www.choicepoint.com)

Zakon Fair and Accurate Credit Transactions (FACT) daje pravo korisnicima na besplatni godišnji izvještaj iz agencija za izvještavanje. Prema ChoicePointu, njegove tri usluge potpadaju pod taj zakon: C.L.U.E., koja prati informacije o povijesti naknada šteta od osiguranja; ChoicePoint WorkPlace Solutions, koja obuhvaća povijest zapošljavanja; Resident Data, koja pokriva povijest stanarina. Nakon stupanja na snagu zakona FACT Act, ChoicePoint mora na zahtjev davati jednu besplatnu kopiju profila vašeg potrošača godine iz svake od ovih poslovnih jedinica. Zapamtite da ove poslovne jedinice možda nemaju vaš potrošački profil. Međutim, ako volite provjeravati, imate na raspolaganju sljedeće adrese www.choicepoint.com i www.choicetrust.com.

10.3 Popis za provjeru

Upotrijebite ovaj popis za provjeru kao brzi referentni vodič kroz gradivo izneseno u ovom poglavlju.

Učinite

- Razmotrite korištenje šifriranja e-pošte da biste zaštitili svoje poruke od njuškala.
- Razmotrite korištenje proizvoda za anonimnost na Webu ili proxyja da biste sakrili svoje surfanje po Webu.
- Svoj matični broj i datum rođenja pokušajte držati podalje od javnih zapisa.
- Provjerite dosjee o sebi koje bi mogli imati glavni mešetari podataka.
- Povucite se iz programa mešetara podataka za dijeljenje informacija gdje god je to moguće.

Nemojte učiniti

- Izostavite osjetljive informacije iz javnih zapisa gdje god je to moguće.
- Nemojte zaboraviti da se vi i ljudi s kojima se dopisujete e-poštom trebate pretplatiti na digitalne certifikate da biste koristili sisteme šifriranja s javnim ključem.

10.4 Korisni izvori

Ovaj odjeljak daje popis dodatnih izvora koji će vam pomoći da saznate više.

Electronic Privacy Information Center (EPIC) javna je interesna grupa za istraživanje koja proučava civilnu slobodu i pitanja privatnosti. Ovaj centar objavljuje izvještaje i knjige o privatnosti, otvorenoj vladi i slobodi govora. Članovi EPIC-a često svjedoče pred državnim i federalnim zakonskim komisijama o privatnosti i zakonodavstvu u vezi s civilnim slobodama. EPIC-ova Web lokacija sadrži gomile novih priča i informacija vezanih uz privatnost. Dvije posebno zanimljive stranice jesu popisi alata za privatnost na Internetu. Posjetite adresu www.epic.org/privacy/tools.html. Zapamtite da EPIC ne prenosi ni jedan od alata s popisa. To je samo ogled dostupnih alata. Trebali biste provjeriti i Top Ten Consumer Privacy Resolutions. Posjetite www.epic.org/privacy/2004tips.html.

Center for Democracy & Technology je neprofitna grupa čija je misija štititi slobodu građana, naročito slobodu govora i privatnost. Članovi CDT-a redovito

svjedoče pred Kongresom o važnim pitanjima poput privatnosti, slobode govora i autorskim pravima. Njezina Web lokacija odličan je izvor informacija o novim zakonima. Na lokaciji ćete pronaći knjige, članke i izvatke iz novina kao i veze za kontaktiranje članova Senata i Gornjeg doma o raznim problemima i pitanjima. Posjetite adresu www.cdt.org.

Electronic Frontier Foundation (EFF) još je jedna neprofitna organizacija koja radi na zaštiti slobode u visoko razvijenom tehnološkom svijetu. EFF prati pitanja kao što su privatnosti, autorska prava, dijeljenje datoteka, e-glasanje itd. Detalje potražite na adresi www.eff.org.

Privacy Rights Clearinghouse je izvor informacija o privatnosti na Internetu, financijskoj privatnosti i drugim temama. Nudi savjete za zaštitu privatnosti i prati federalne zakone koji se odnose na privatnosti. Posjetite www.privacyrights.org.

U Hrvatskoj je nemoguće obratiti se nekoj državnoj, stručnoj ili neprofitnoj organizaciji koja može pomoći savjetima ili mehanizmima za zaštitu od opasnosti koje vrebaju s Interenta – jednostavno zato što takve organizacije (još) ne postoje. S druge strane, one organizacije koje postoje a usmjerene su na zaštitu potrošača još se nose sa mnogo primitivnijim (ali i češćim) napadima na sigurnost i novčanik građana. Za masovne napade prevaranata morat ćemo pričekati dok ne budemo malo bogatiji – a informatička struktura prodre u svaku poru našeg društva. No, da bi naš prosječni korisnik računala bio dobro zaštićen pri svojim Internetskim aktivnostima, on treba saznati više, a to može, naravno, na Internetu. Jedan od vrlo efikasnih načina je predbilježiti se na news grupu hr.comp.sigurnost, gdje se trenutno pojavljuju spoznaje o opasnostima koje nas vrebaju, a svaki gost može postaviti pitanja stručnjacima koji će na njih odgovoriti po parlamentarnim načelima. Povrh toga, naši informatički časopisi uistinu su vrijedni čitanja; pružaju informacije o novim sigurnosnim proizvodima, njihove recenzije i usporedne testove, a postoje i dobre stare rubrike "pisma čitatelja". Naravno, kako nitko ne puše na hladno, i vi zacijelo nećete tražiti pomoć zato što ste iznenada postali svijesni opasnosti, već zato što vam se računalo neobično ponaša, samo se spaja na Internet, sustav se ruši, gubite datoteke ili računalo postaje sporo. Teško da ćete ikakvim alatom popraviti problem – to je posao za stručnjaka. Alati održavaju računalo u dobrom stanju – ukoliko je početno stanje bilo dobro. Kako na svom automobilu ne želite sami popravljali elektorniku – a ne biste to prepustili ni klincu iz kvarta, tako se za sigurnosna pitanja na vašem računalu trebate obratiti stručnjaku.

op.red.

Zaključak

Hvala vam što ste pročitali ovu knjigu. Nadamo se da smo vam pomogli da shvatite koji su rizici vezani uz sigurnost na Internetu i da smo vam pružili neke praktične informacije o načinima na koji sebe i svoju obitelj možete zaštititi dok ste *online*.

Surfanje Webom može biti jednako sigurno kao i šetnja kvartom. Uz prave alate i poduku moći ćete izbjeći mnoge zamke i opasnosti koje vode do financijskih gubitaka, gubitaka podataka i narušavanja performansi računala, ili samo gubitka živaca.

Danas *spyware*, *spam* i Internetske prijevare pune naslovnice novina. No tehnologija se stalno mijenja pa će budućnost donijeti nove rizike i prijetnje zajedno s najnovijim softverom i novima "guba" mogućnostima. Dobra je vijest to što se većina praktičnih savjeta u ovoj knjizi može primijeniti na nove prijetnje te na rizike o kojima smo govorili u prethodnim poglavljima.

Ovdje se, kao mali podsjetnik, nalazi pet osnovnih koraka koje možete poduzeti da biste svoje računalo zaštitili od sadašnjih i budućih napada:

1. Upotrijebite neko sigurnosno Internetsko rješenje koje kombinira upravljanje antivirusnim i *anti-spyware* softverom, vatrozidom, otkrivanjem provala i pukotinama u korisničkom softveru da biste postigli maksimalnu zaštitu od prikrivenih prijetnji. Svoju sigurnosnu uslugu redovito ažurirajte da biste imali trenutne definicije virusa/*spywarea*.

2. Redovito ažurirajte softver svojeg operativnog sustava i Web pretraživača. Zapamtite da je svaki drugi utorak u mjesecu *Utorak zakrpa*, kada Microsoft objavljuje najnovije ispravke svojeg softvera. Neka vam postane navika da dohvaćatte i instalirate te ispravke na vrijeme ili uključite funkciju Automatic Updates u Windowsima XP. Svakako koristite lozinke koje kombiniraju brojke i slova.
3. Ne uzimajte slatkiše od stranaca. Pod tim mislimo da biste morali biti sumnjičavi, ili barem oprezni, prilikom korištenja Interneta. Budite posebno oprezni s "besplatnim" programima koji obećavaju nešto zabavno ili korisno. Budite vrlo sumnjičavi kod dolazne e-pošte. Ne otvarajte poruke koje šalju ljudi koje ne poznajete. Ako te poruke ipak otvarate, nemojte slučajno aktivirati ili preuzeti ili kliknuti ni na jedan prilog koji je došao s takvom porukom. Nikome nikada ne šaljite osjetljive informacije u porukama e-pošte, kao što su lozinke, brojevi kreditnih kartica ili bankovnih računa.
4. Ne kupujte ništa od *spamera*. Imajte na umu opasnosti koje su vezane uz kupnju softvera – ili bilo kojeg proizvoda – koji se nudi u *porukama* e-pošte. Taj bi softver mogao sadržavati viruse ili bugove koji bi mogli biti vrlo destruktivni za operativni sustav vašeg računala. Ne pretplaćujte se na nepoznate Web lokacije koje obećavaju da će vaše ime ukloniti sa *spam* popisa i nemojte klikati na veze "remove from mailing list" u *porukama* e-pošte; to su trikovi koje *spameri* koriste da bi provjerili i dobili *adrese* e-pošte.
5. Redovito snimajte sigurnosne kopije važnih datoteka da biste spriječili gubitak podataka u slučaju ozbiljnog problema s računalom. Datoteke možete spremati na CD-ove ili memorijske kartice, ili *možete koristiti online* uslugu pohranjivanja.

Ako vam je ovih pet pravila previše, možemo iz njih izvesti jedno: *koristite zdrav* razum. Internet nije vaš prijatelj. To je zajednica, kao i svaka druga, u kojoj određeni postotak čine lopovi, kriminalci, prevaranti i huligani. To nikako ne znači da izbjegavate korištenje Interneta; samo se krećite po njemu kao što biste se kretali po nepoznatom dijelu grada – držite oči širom otvorene, koristite svoj mozak i čuvajte svoj novčanik.

Kazalo

Simboli

180Solutions, 73
802.11a IEEE, standard, 175-176
802.11b IEEE, standard, 175-176
802.11g IEEE, standard, 175-176
802.1x IEEE, standard, 175
911, VoIP, sigurnost, 191

A

AAC (Advanced Audio Coding), 166
Acohido, Byron, 120
ActiveScan Pro, 84
ActiveX kontrole, 89, 132-136
Acxiom Web lokacija, 206
Ad-Aware SE Personal, 87
Ad-Aware SE Plus, 83-84
Add a Port, dijaloški okvir, 126
Add a Program, dijaloški okvir, 125
Advanced Audio Coding (AAC), 166
Advanced Encryption Standard (AES), 197
Advanced kartica, Windows Firewall, 126
adware, 4-5
  definiranje, 67-72
  izvori, 96
  kako inficira računalo, 80-82
  otkrivanje, 72-78
  poželjne i nepoželjne aktivnosti, 95-96
  uklanjanje, 92-95
  zaštita protiv
    alternativni pretraživači, 91
    anti-spyware softver, 87-88
    besplatni anti-spyware softver, 86-87
    EULA (End User License Agreement), 89
    Internet Sigurnost, opcije, 89, 91
    pazite da inferioran antivirusni softver, 85
    pazite na besplatan softver, 88
    ažurirani softver, 91-92
AES (Advanced Encryption Standard), 197
alati, sprječavanje krađe identiteta, 15-16
alternativni pretraživači, 91, 158
American Online (AOL), 18
Andreessen, Marc, 31
anonymizer, Web, 204-205
Anti-Phishing Working Group (APWG), Web lokacija, 22
Anti-Spam Personal, 116
anti-spam, alati, 115-117
anti-spyware softver, 15-16, 82-85
  besplatan softver, 86-87
  ograničenja, 88
  skeniranje računala, 92-93
  sposobnosti, 87-88

Anti-Virus Personal, 61
antivirus
  nadziranje, ZoneAlarm, 40
  softver, 15-16, 54, 82-85
    inferiorni proizvodi, 85
    odabir, 60-62
    ograničenja, 54-56
    skeniranje računala, 92-93
    sposobnosti, 54
AOL (American Online), 18
AP (pristupna točka), 174
APWG (Anti-Phishing Working Group), Web lokacija, 22
asimetrično šifriranje, 197-198
AuditMyPC, 45
Automatic Updates,
  dijaloški okvir, 131
  Windows XP Service Pack 2, 39, 122, 130-131
AV softver. *Vidi* antivirusni softver
Avenue Media, 73
AVG Anti-Virus, 61
ažuriranja
  automatska, Windows XP Service Pack 2, 39, 130-131
  softvera, 91-92

B

Bayesian, filter, 110-111
Beagle.BA, crv, 63-66
Belkin, 174
Bellekom, Merijn, CWShredder, 87
Berners-Lee, Tim, 31
besplatan softver, 86-88
bežična tehnologija, 173
  izvori, 192
  mobilni telefoni, 185-189
  mreže, 174-182
  PDA-ovi, 185-190
  poželjne i nepoželjne aktivnosti, 192
  sigurnost javnih vrućih točki, 182-185
  VoIP sigurnost, 190-191
BHO (Browser Helper Object), 72
bijele liste, *spam* filter, 108
Black ICE PC Protection, 42
BlackBerrys, 173
Blaster, crv, 4, 52
Bluetooth, 186-189
Bonded Sender, program, 111
Bono, Mary, SPY ACT, 76
Boxer, Barbara, SPY BLOCK Act, 76
brokeri podataka, 205
  Acxiom, 206
  ChoicePoint, 206-207
Browser Helper Object (BHO), 72
Bugbear, crv, 52
bugovi, Web, 106
Burns, Conrad, SPY BLOCK Act, 76

C

California Senate Bill 1386, 22-23
Cascade, virus, 51
CastleCops, Web lokacija, 85, 94, 144
Center for Democracy and Technology, Web lokacija, 204
certifikati, digitalni, 199-200
Chatter: Dispatches from the Secret World of Global Eavesdropping, 210
ChoicePoint Consumer Disclosure Center, 207
  incident, 23
  Web lokacija, 206-207
ChoicePoint WorkPlace Solutions Consumer Disclosure Center, 207
Claria, 73
Clark, Jim, Netscape Navigator, Web pretraživač, 31
Cloudmark SafetyBar 4.0, 116
Cloudmark, 111
CNET, Web lokacija, 62
Computer Associates, eTrust PestPatrol, 83
Concept, virus, 51
Content Advisor
  dijaloški okvir, 155-156
  Internet Explorer, 153
ContentProtect, 165
ContentWatch Web lokacija, 165
CoolWebSearch, *adware*, 86
CounterSpy, 83-84
crne liste, *spam* filter, 108
crvi, 4, 50-52
  antivirusni softver, 54-56
  Beagle.BA, 63-66
  izvori, 62-63
  odabir antivirusnog softvera, 60, 62
  oporavak od zaraze, 59-60
  poželjne i nepoželjne aktivnosti, 62
  sposobnosti, 53
  zaštita od 56-58
CWShredder, 86-87
CyberPatrol, 165
CYBERSitter, 165

D

datoteke
  dijeljenje, 164-169
  šifriranje, 203-204
  zaraženi virusi, 51
dialeri, 72
Digital ID, 203
Digital Subscriber Line (DSL), 29
digitalni certifikati, 199-200
digitalni potpisi, 199-200
Direct Revenue, 73
djeca, aktivnost na Internetu, 147-148
  dijeljenje datoteka, 164-169
  filtriranje sadržaja, 148-160
  izvori, 170-171
  poželjne i nepoželjne aktivnosti, 170
  seksualni grabežljivci, 160-165
dječje Web lokacije, 159
D-Link, 174
dnevnici
  vatrozidovi, 34
  ZoneAlarm, 40-41
Download.ject, trojanski konj, 132
društveni inženjering
  metoda krađe identiteta, 11-12
  spam, 106
  zaraza nepoželjnim softverom, 82
DSL (Digital Subscriber Line), 29

E

eEye, 129
EFF (Electronic Frontier Foundation), Web lokacija, 204, 209
Electronic Privacy Information Center (EPIC), 205, 209
End User License Agreement (EULA), 89
Enhanced Consumer Protection Against Spyware Act of 2005, 76
EnoLogic, 165
EPIC (Electronic Privacy Information Center), 205, 209
e-pošta
  krađa identiteta, 11-12
  phishing napadi, 12-13
  spam, 3, 101-118
  šifriranje, 200-203
  virusi, zaštita od, 57-58
  zaraza nepoželjnim softverom, 82
  ZoneAlarm, 40
Equifax, 15
eTrust
  Antivirus, 61
  EZ Armor, 42
  PestPatrol, 83-86
EULA (End User License Agreement), 89
Exceptions kartica, Windows Firewall, 124
Experian, 15
Explorer
  filtri sadržaja, 153-158
  pronalaženje povijesti, 149

F

FACT Act, 206
FACT Act: C.L.U.E., 206
Fair and Accurate Credit Transactions (FACT) Act, 206
Family Entertainment and Copyright Act, 167
filmovi, problemi s dijeljenjem datoteka, 164, 166-167
  legalno nasuprot ilegalnom, 169
  lociranje kršitelja autorskih prava, 168
  P2P sigurnosni rizici, 168-169
filtri
  Internet sadržaja, 148-149
    alternativni pretraživači, 158
    Explorer, 153-158
    kontrola spama, 159-160
    kontrole davatelja usluga, 158-159
    ručno nadziranje, 149, 151
    tražilica, 151-153
  spam, 106-107
    Bayesian, 110-111
    bijele liste, 108
    crne liste, 108
    heurističke analize, 108-109
    izazov/odziv sistem, 110
    potpisi, 109-110
    reputacije, 111-112
    sadržaj, 107
filtriranje po reputaciji, *spam*, 111-112
Firefox, 120, 140-141
  filtriranje sadržaja, 158
  pregledavanje povijesti, 151
  preuzimanje, Web lokacija, 91
Firewall Guide, Web lokacija, 46
F-Secure
  Anti-Virus, 61
  Anti-Virus for Pocket PC, 188
  Internet Security, 42
  Mobile Anti-Virus, 188
FTC, Web lokacija, 21

G

GAIN, 73
Gator, 73
Gibson, Steve, ShieldsUP!, 44, 142
glazba, problemi s dijeljenjem datoteka, 164-167
  legalno nasuprot ilegalnom, 169
  lociranje kršitelja autorskih prava, 168
  P2P sigurnosni rizici, 168-169
gmizavci, *spam* e-pošte, 104
Gnutella, 166
Gobi, virus, 51
Goodlatte, Bob, I-SPY Prevention Act of 2005, 76
grabežljivci, 160
  prijavljivanje, 162
  softver za nadziranje, 162-165
  sprječavanje kontakta, 161-162
GriSoft, 61
Grokster, 166

H

Happy99 mailer, 52
heuristička analize, *spam* filter, 108-109
Hicks, Matt, 77
HijackThis, 85-87, 93-94
Hilden, Julie, 171
HIPS (Host Intrusion Prevention Solutions), 55
Host Intrusion Prevention Solutions (HIPS), 55
HotSpotVPN, Web lokacija, 184
HTML (Hypertext Markup Language), 30-31
HTTP (Hypertext Transfer Protocol), 16, 30-31
Hypertext Markup Language (HTML), 30-31
Hypertext Transfer Protocol (HTTP), 16, 30-31

I

ICMP (Internet Control Message Protocol), 127
ICRA (Internet Content Rating Association), 153
Identity Theft Resource Center, Web lokacija, 22
IEEE (Institute of Electrical and Electronics Engineers), 28, 174-175
IETF (Internet Engineering Task Force), 28
InfoBase i Sentricx Reference, 206
InfoBase Marketing, 206
Information Bar, Windows XP Service Pack 2 (SP2), 135-136
Institute of Electrical and Electronics Engineers (IEEE), 28, 174-175
Internet Content Rating Association (ICRA), 153
Internet Control Message Protocol (ICMP), 127
Internet Crime Complaint Center, Web lokacija, 21
Internet Engineering Task Force (IETF), 28
Internet Explorer
  ActiveX kontrole, 132-136
  filtri sadržaja, 153-158
  izvori, 144-145
  Pop-Up Blocker, 138-139
  postavke za privatnost, 136-137
  poželjne i nepoželjne aktivnosti, 144
  sigurnost, 132
  verzija 7.0, 143
Internet Options, dijaloški okvir, 133, 154
Internet Protocol (IP), 29-30
Internet Security Suite, 42
Internet Service Providers (ISP-ovi), 158-159
Internet, 147-148
  dijeljenje datoteka, 164-169
  filtriranje sadržaja, 148-160
  izvori, 170-171
  poželjne i nepoželjne aktivnosti, 170
  seksualni grabežljivci, 160-165
  sigurnost, koraci za, 211-212
  sigurnost, opcije, 89-91
IP (Internet Protocol), 29-30
ISP (Internet Service Provider), 158-159
ispitivači penetracije, 11
I-SPY Prevention Act of 2005, 76
izazov/odziv sustav, *spam* filter, 110
izlazne veze, vatrozidovi, 31, 33
izvori
  adware, 96
  bežična tehnologija, 192
  Internet aktivnost, 170-171
  krađa identiteta, 21-22
  privatnost, 209-210
  spam, 118
  spyware, 96
  trojanski konji, 96
  vatrozidovi, 46
  virusi i crvi, 62-63

J

Jaynes, Jeremy, 101
Jerusalem, virus, 51

K

karantene, 59, 87
Kaspersky AntiVirus Personal, 188
Kaspersky Personal Security Suite, 42
Kazaa, 73, 97, 166
Kerio Personal Firewall, 43
keylogger, 71
keystroke loggeri, 13, 71
kolačići za praćenje, 78
kolačići, uklanjanje, 78-80
konfiguracije, Windows Firewall, 124-127
kopanje po smeću, metoda krađe identiteta, 14
krađa identiteta, 3, 9-10
  izvori, 21-22
  načini, 10-14
  oporavljanje, 19-20
  osobno iskustvo autora, 24-25
  poželjne i nepoželjne aktivnosti, 20-21
  sprječavanje, 14-19

L

legalno
  Internet dijeljenje datoteka, 169
  uklanjanje nepoželjnog softvera, 72-78
Libin, Phil, SpoofStick, 19
Linksys, 174
Linux, 120
LookSmart, Web lokacija, 165
LoveLetter (masovni mailer), 52
lozinke, WLAN-ovi, 180
LucidLink Wireless Security, 182

M

MAC filtriranje, 180-181
Macintosh, 120
Mail Abuse Prevention System (MAPS), 108
mailer, crvi, 52
MailFrontier Desktop, 116
makro virusi, 51
malware, 2-5
  mobilni telefoni, 187-188
  razlozi za cvjetanje, 47-50
mape, šifriranje, 203-204
MAPS (Mail Abuse Prevention System), 108
Marburg, virus, 51
Markoff, John, Takedown: The Pursuit and Capture of Kevin Mitnick, 12
mas-mailing, crvi, 52
McAfee, 60
  anti-spyware, 84
  MySecurityStatus, 44
  Web lokacija, 59
  Wi-Fi Scan, 181
međunarodna lutrija, 102
Melissa, virus, 51
Message Options, dijaloški okvir, 201
MGM Studios, Inc. nasuprot Grokster, LTD, 167
Michelangelo, virus, 51
Microsoft AntiSpyware, 86-87
Microsoft Internet Explorer. *Vidi* Internet Explorer
Microsoft Windows. *Vidi* Windows
Microsoft, Web lokacija, 144
Mitnick, Kevin, društveni inženjer, 11
mobilni telefoni, 173, 185-186
  Bluetooth, 186-189
  malware, 187-188
Morpheus, 166
Motion Picture Association of America (MPAA), 166
MPAA (Motion Picture Association of America), 166
mreže za izravnu razmjenu podataka (P2P mreže),
  dijeljenje datoteka, 164-167
  legalno nasuprot ilegalnom, 169
  lociranje kršitelja autorskih prava, 168
  sigurnosni rizici, 168-169
mreže, bežične
  izvori, 192
  mobilni telefoni, 185-189
  PDA-ovi, 185-190
  poželjne i nepoželjne aktivnosti, 192
  problemi sa sigurnošću, 175-182
  sigurnost javnih vrućih točki, 182-185
  sposobnosti, 174-175
  VoIP sigurnost, 190-191
MyDoom, crv, 52

N

nadziranje
  Internet aktivnosti, 149-151
  programi, ZoneAlarm, 40
  seksualni grabežljivci, 162-165

napadi, pecanje, metoda krađe identiteta, 12-13
Napster, 166
National Center for Missing and Exploited Children, Web lokacija, 162
NetGear, 174
NetNanny, 165
Netscape Navigator, Web pretraživač, 31
Netsky, crv, 52
nigerijska nafta, prijevara, 102
Nimda, crv, 52-53, 130
No Place to Hide: Behind the Scenes of Our Emerging Surveillance Society, 210
NOD32, 61
Norton AntiSpam, 116
Norton AntiVirus, 60-61
Norton Internet Security, 33, 42

O

obitelj, aktivnost na Internetu, 147-148
  dijeljenje datoteka, 164-169
  filtriranje sadržaja, 148-160
  izvori, 170-171
  poželjne i nepoželjne aktivnosti, 170
  seksualni grabežljivci, 160-165
OnlyMyEmail Personal, 117
Opera, 120, 141-142
  filtriranje sadržaja, 158
  pregledavanje povijesti, 151
  pretraživač, preuzimanje, Web lokacija, 91
operativni sustavi. *Vidi i* Windows
  izvori, 144-145
  osiguravanje, 119-121
  sigurnosne provjere, 142-143
  Vista, 143
oporavci, virusi, 59-60
osnove kriptografije, 197-198
osobni digitalni pomoćnik. *Vidi* PDA
osobni identifikacijski brojevi (PIN-ovi), 17
otmice, 2
  adware, 4-5
  crvi, 4
  krađa identiteta, 3
  razlozi za, 5-7
  spam, 3
  spyware, 4-5
  trojanski konji, 4-5
  virusi, 4

P

P2P mreže (mreže za izravnu razmjenu podataka),
  dijeljenje datoteka, 164-167
  legalno nasuprot ilegalnom, 169
  lociranje kršitelja autorskih prava, 168
  sigurnosni rizici, 168-169
paketi, 28-31
Palm Piloti, 173
PalmOS, 186
Panda Platinum Internet Security 2005, 117
Panda Platinum Internet Security, 42
Panda Software Web, lokacija, 59
PAN-ovi (Personal Area Networks), 186
PassCode, 18
PayPal e-pošta, 103
PC Magazine Web lokacija, 62
PC World Web lokacija, 62
PC-cillin for Wireless, 188
PC-cillin Internet Sigurnost, 42, 117
PC-cillin, 60-61, 84, 182
PDA-ovi (osobni, digitalni pomoćnici), 173, 185-186
  Bluetooth, 186-189
  malware, 187-188
  osiguravanje, 188-190
Personal Area Network (PAN), 186
Pew Internet, Web lokacija, 118
PGP (Pretty Good Privacy), 200-203
phishing, 12-13, 102-104
PIN-ovi (osobni identifikacijski brojevi), 17-18
PivX PreView, 45, 142-143
Pocket PC, 186
polimorfni virusi, 51
Pop-Up Blocker, 138-139
portovi, 28-31
postavke za privatnost, Internet Explorer, 136-137
pošta, metoda krađe identiteta, 14
potpisi
  digital, 199-200
  spam filter, 109-110
povijest, Internet Explorer, 149-150
povreda autorskih prava, lociranje, 168
prelijevanje međumemorije, Windows XP Service Pack 2, 128
pretraživači. *Vidi i* Internet Explorer
  alternative, 91, 139-142, 158
  izvori, 144-145
  otimač, 71

sigurnost, opcije, 89-91
SpoofStick, 18-19
zaraza nepoželjnim softverom, 80-81
pretraživanja po ključnoj riječi, filtriranje *spama*, 107
pretraživanje sadržaja, filtriranje *spama*, 107
Pretty Good Privacy (PGP), 200-203
preuzimanja
problemi s dijeljenjem datoteka, 164-169
vatrozidovi, 36-41
prijavljivanje, Internet seksualnog vabljenja, 162
prijenosni uređaji, 185-186
Bluetooth, 186
malware, 187-188
osiguravanje Bluetootha, 188-189
osiguravanje PDA-ova, 189-190
prijetnje, 2
adware, 4-5
crvi, 4
krađa identiteta, 3
razlozi za, 5-7
spam, 3
spyware, 4-5
trojanski konji, 4-5
virusi, 4
prijevara, 2
adware, 4-5
crvi, 4
krađa identiteta, 3
razlozi za, 5-7
spam, 3
spyware, 4-5
trojanski konji, 4-5
virusi, 4
prijevare s kreditnim karticama, 10
prijevare, 102-104
prilozi, zaštita od virusa, 58
pristupna točka (AP), 174
Privacy Rights Clearinghouse, Web lokacija, 209
privatnosti, 195-197
brokeri podataka, 205-208
izvori, 209-210
opcije, 197-205
poželjne i nepoželjne aktivnosti, 208
Privoxy, Web lokacija, 204
protokoli, 28-31
provjera valjanosti s dva faktora, 17-18
provjera valjanosti, sprječavanje krađe identiteta, 17-18
proxiji, spam, 105-106
PSAP (Public Service Answering Point), 191
Public Service Answering Point (PSAP), 191

R

RAT (Remote Access/Administration Tool), 72
Rating Systems, dijaloški okvir, 156
RBL (Realtime Blackhole List), 108
Realtime Blackhole List (RBL), 108
Recording Industry Association of America (RIAA), 164
Recreational Software Advisory Council (RSACi), 153
Remote Access/Administration Tool (RAT), 72
Resident Data Consumer Disclosure Center, 207
retro virusi, 51
rezidentni u memoriji, virusi, 51
RIAA (Recording Industry Association of America), 164
rječnik napadi, 104-105
RSACi (Recreational Software Advisory Council), 153

S

SafeSurf, 154
scavengers, *spam* e-pošta, 104
Schneier, Bruce, *Secrets and Lies: Digital Security in a Networked World*, 46
SearchScout, 77
Secrets and Lies: Digital Security in a Networked World, 46
Secunia, 129, 145
Secure Socket Layer (SSL), 16
SecurID token, 17
Security kartica, Internet Options, dijaloški okvir, 133
seksualni grabežljivci, 160
nadziranje, softver, 162-165
prijava vabljenja, 162
sprječavanje kontakta, 161-162
Service Set Identifier (SSID), 180
ShieldsUP!, 44, 142
Shimomura, Tsutomu, *Takedown: The Pursuit and Capture of Kevin Mitnick*, 12
SIG (Special Interest Group), 186
Sigurnost Center, 121-123
Sigurnost Properties, dijaloški okvir, 202
Sigurnost Settings, dijaloški okvir, 90, 134

sigurnost
koraci za, 211-212
postavke vatrozida, 33-35
tokeni, 17-18
WLAN-ovi, 175-182
simetrično šifriranje, 197-198
skeniranja, zaraze virusima, 59
skrivene prijetnje, 52
Slammer, crv, 52-53
sniferski, alati, 176
softver
ažurirane verzije, 91-92
Internet nadziranje, 163-165
WLAN-ovi, 181-182
zaraza nepoželjnim softverom, 81
zaštita od virusa, 58
Solid Oak Software, Web lokacija, 165
Sony protiv Universal Studios, 167
Sorkin, David, 118
Spam Filter Express, 117
spam, 3, 99-100
anti-spam alati, 115-117
filtriranje sadržaja, 159-160
izvori, 118
metode filtriranja, 106-112
metode, 104-106
osnove, 101-102
phishing, 102-104
poželjne i nepoželjne aktivnosti, 117-118
prijevare, 102-104
smanjivanje, 112-115
SpamAssassin, Web lokacija, 109
SpamCop, Web lokacija, 108, 118
spameri, *spoofiranje* vraćene e-pošte, 12
SpamHause, Web lokacija, 108
SpamKiller, 117
Spamroll, Web lokacija, 118
Special Interest Group (SIG), 186
spoofing, 12, 105
SpoofStick, sprječavanje krađe identiteta, 18-19
SPY ACT, 76
SPY BLOCK Act, 76
Spy Sweeper, 83-84
Spybot Search&Destroy, 86-87
SpyCatcher, 83-84
spyware, 4-5
Assassin, 85
definiranje, 67-72
eliminator, 84
izvori, 96
kako inficira računalo, 80-82
otkrivanje, 72-78
poželjne i nepoželjne aktivnosti, 95-96
uklanjanje, 92-95
Warrior, Web lokacija, 94
zaštita od 82-92
SpywareInfo, Web lokacija, 85
SQL Slammer, 4
SSID (Service Set Identifier), 180
SSL (Secure Socket Layer), 16
standardi, IEEE (Institute of Electrical and Electronics Engineers), 174-175
Sunbelt Software, CounterSpy, 83
SurfControl, Web lokacija, 165
Sutton, Willie, 119
Swartz, Jon, 120
Sygate Personal Firewall Pro, 42
Sygate Personal Firewall Standard, 43
Symantec
AntiVirus for Handhelds, 188
Norton AntiVirus, 60
Security Check, 44, 59, 143
Spyware Edition, 84
studija nepoželjnog softvera, 73
Mobile Security 4.0, 188

Š

šifriranje, 197-198
datoteke, 203-204
e-pošta, 200-203

T

Takedown: The Pursuit and Capture of Kevin Mitnick, 12
TCP (Transmission Control Protocol), 29-30
telefonska prijevara, 21
Tenebril, SpyCatcher, 83
testiranje, vatrozidovi, 44-45
Thomas Web lokacija, 77
tipkovnice, *keystroke loggeri*, 13
Titanium Antivirus, 61
tokeni, sigurnost, 17-18
Transmission Control Protocol (TCP), 29-30
TransUnion, 15
tražilice, filtri, 151-153
Trend Micro, 60
House Call, 59
Mobile Security, 188
Wi-Fi Intrusion Detection, 182
trojanski konji, 4-5
definiranje, 67-72
izvori, 96

kako inficiraju računalo, 80-82
poželjne i nepoželjne aktivnosti, 95-96
uklanjanje, 92-95
zaštita od 82-92
Trusted Sites, 134
tvrdi diskovi, ponovno formatiranje, 95

U

ulazne veze, vatrozidovi, 31-33
upozorenja, ZoneAlarm, 40-41
usmjernici, bežični, 174

V

vatrozidovi, 27-28
besplatna preuzimanja, 36-41
izvori, 46
kupovina, 41-42
odabir, 43
ograničenja, 35-36
poželjne i nepoželjne aktivnosti, 45-46
protokoli, 28-31
sposobnosti, 31-35
testiranje, 44-45
Windows, 122-127
zaštita od virusa, 56-57
VeriSign, digitalni ID, 203
veze, vatrozidovi, 31-33
Virtual Private Network (VPN-ovi), 184
Virus Bulletin, Web lokacija, 62
Virus List, Web lokacija, 62
virusi sektora za podizanje računala, 51
virusi, 4, 50-52
antivirusni softver, 54-56
Beagle.BA, 63-66
izvori, 62-63
odabir antivirusnog softvera, 60, 62
oporavak od zaraze, 59-60
poželjne i nepoželjne aktivnosti, 62
sposobnosti, 53
Windows XP Service Pack 2, 39, 127-128
zaštita od 56-58
VirusScan, 60-61
Visa, Web lokacija, 21
Vista operativni sustav, 143
Voice over IP. *Vidi* VoIP
VoIP (Voice over IP), 29, 173
bežične mreže, 174-182
izvori, 192
poželjne i nepoželjne aktivnosti, 192
sigurnost, 190-191
VPN (Virtual Private Network), 184

W

Web lokacija, 39
Web lokacije
Acxiom, 206
Anti-Phishing Working Group (APWG), 22
AuditMyPC, 45
CastleCops, 85, 94, 144
Center for Democracy and Technology, 204
Childrens Internet, 159
ChoicePoint, 206-207
CNET, 62
ContentWatch, 165
CWShredder, 87
EFF (Electronic Frontier Foundation), 209
Electronic Frontier Foundation (EFF), 204
EnoLogic, 165
EPIC (Electronic Privacy Information Center), 209
Firewall Guide, 46
FTC, 21
HijackThis, alat, 85
HotSpotVPN, 184
Identity Theft Resource Center, 22
Internet Crime Complaint Center, 21
Kazaa, 97
LookSmart, 165
Mail Abuse Prevention System, 108
McAfee MySecurityStatus, 44
McAfee, 59
Microsoft, 144
Mozilla, 140-141
National Center for Missing and Exploited Children, 162
Opera, 141-142
Panda Software, 59
PC Magazine, 62
PC World, 62
Pew Internet, 118
PivX PreView, 45, 142-143
Privacy Rights Clearinghouse, 209
Privoxy, 204
ShieldsUP!, 44, 142
Solid Oak Software, 165
SpamAssassin, 109
SpamCop, 108, 118
SpamHause, 108
Spamroll, 118
spoofing, 12
SpoofStick, 18-19
Spyware Warrior, 94
SpywareInfo, 85
SurfControl, 165
Symantec Security Check, 44, 59, 143
Thomas, 77
Trend Micro, 59
Virus Bulletin, 62
Virus List, 62

Visa, 21
WildList Organization, 63
Zone Labs, 39
Web, 147-148
anonymizer, 204-205
bugovi, 106
dijeljenje datoteka, 164-169
filtriranje sadržaja, 148-160
izvori, 170-171
koraci za sigurnost, 211-212
poželjne i nepoželjne aktivnosti, 170
pretraživači. *Vidi* pretraživači
seksualni grabežljivci, 160-165
Webroot Software, Spy Sweeper, 83
Welcome to Secure E-mail, dijaloški okvir, 202
WEP (Wired Equivalent Privacy), 177
WhenU., 73
Wi-Fi (wireless fidelity), 174
izvori, 192
mobilni telefoni, 185-189
mreža, sposobnosti, 174-175
otkrivanje provale, 182
PDA-ovi, 185-190
poželjne i nepoželjne aktivnosti, 192
sigurnost javnih vrućih točki, 182-185
VoIP sigurnost, 190-191
WLAN-ovi, problemi sigurnosti, 175-182
Wi-Fi Protected Access (WPA), 177
WildList Organization, Web lokacija, 63
Windows, 119-121
Firewall, 122
izvori, 144-145
poželjne i nepoželjne aktivnosti, 144
Security Center, 37
sigurnosne provjere, 142-143
Vista,operativni sustav, 143
Windows XP Service Pack 2 (SP2), 36-37, 43, 121
automatska ažuriranja, 39
besplatni vatrozid, 37-39
konfiguracija vatrozida, 124-127
prelijevanje međumemorije, 128
Security Center, 121-123
Wireless Network Setup Wizard, 178
zakrpe, 128-131
zaštita od virusa, 39, 127-128
Wired Equivalent Privacy (WEP), 177
wireless fidelity. *Vidi* Wi-Fi
Wireless Local Area Networks (WLAN-ovi), 175
Wireless Network Setup Wizard, 178
WLAN (Wireless Local Area Network), 175
WPA (Wi-Fi Protected Access), 177
WPA2, 177
Wyden, Ron, SPY BLOCK Act, 76

X

X-Force, 129

Y

Yahoo!, *anti-spyware* softver, 86

Z

zakoni, uklanjanje nepoželjnog softvera, 72-78
zakrpe, Windows XP Service Pack 2 (SP2), 128-131
zao blizanac, napadi, 185
Zimmermann, Phil, PGP (Pretty Good Privacy), 200
Zmist, virus, 51
Zone Labs
ZoneAlarm, 39-41
ZoneAlarm, 39-43
AntiVirus, 6
antivirusni nadzor, 40
dnevnici, 40-41
program za nadziranje, 40
Security Suite, 42, 117
upozorenja, 40-41
vatrozidovi, 40
Wireless Security, 182
zaštita e-pošte, 40

Ž

žetva imenika, 104-105

Rječnik

Engleski pojam	Prijevod	Objašnjenje
adware		Program koji prati vašu *online* aktivnost i te podatke šalje marketinškoj ili oglasnoj agenciji; neki *adware* programi koriste te podatke za postavljanje zamjenskih oglasa na Web lokacije.
anonymizer		Anonymizer (naziva se i Web anonymizer) je usluga za privatnost koja omogućuje anonimno pretraživanje Interneta i komuniciranje e-poštom.
anti-virus softeware	antivirusni softver	Softver koji skenira i čisti viruse iz računalnog sustava.
authentication	provjera valjanosti	Postupak određivanja je li netko ili nešto ono za što se predstavlja da jest.
backdoor	stražnja vrata	Priswtupni smjer za ulazak u računalni sustav bez dopuštenja korisnika.
banner ad	baner	Grafička reklama na Web stranici.
biometrics	biometrika	Znanost o mjerenju i analiziranju bioloških karakteristika kao što je otisak prsta, slika mrežnice, boja glasa, crte lica itd.
black list	crna lista	Popis određenih Internet adresa i domena za koje se zna da generiraju *spam* poruke.

Engleski pojam	Prijevod	Objašnjenje
boot sector virus	virus sektora za podizanje računala	Virus koji inficira particiju diska ili disk koji se koristi za podizanje računalnog sustava.
browser helper object (BHO)		Mali program koji se legitimno povezuje s korisnikovim pretraživačem Interneta.
buffer overflow	prelijevanje međumemorije	Do prelijevanja međumemorije dolazi kada neki program ili proces pokušava u međumemoriju pohraniti više podataka (privremeno mjesto za pohranjivanje podataka) nego što međumemorija može primiti. Budući da su međumemorije kreirane tako da sadrže konačnu količinu podataka, prekomjerne informacije mogu se preliti u susjedne međumemorije, oštećujući ili prepisujući se preko važećih podataka koji su privremeno u njima pohranjeni. Iako se to može slučajno dogoditi zbog pogreške u programiranju, prelijevanje međumemorije vrlo je uobičajena vrsta napada na integritet podataka. U tim napadima, prekomjerni podaci mogu sadržavati kodove namijenjene pokretanju specifičnih akcija, koje šalju nove upute napadnutom računalu i koje, primjerice, mogu oštetiti datoteke korisnika, promijeniti podatke ili otkriti tajne informacije.
Carnivore		Paket sniferskih programa koji koristi i FBI za špijuniranje kriminalaca i terorista.
certificate authority	certifikacijski autoriteti	Pouzdane tvrtke koje izdaju digitalne certifikate.
code signature	kôd virusa	Dijelovi binarnog koda koji su uvijek jednaki u nekom računalnom virusu.
computer hijacking	otmica računala	Napad prilikom kojeg napadač preuzima kontrolu nad računalom, obično preko trojanskog konja, da bi napao neko drugo računalo ili mrežu.
content filter	filter sadržaja	Program koji analizira Web stranice i blokira pristup stranicama s nedoličnim sadržajem.
cookie	kolačić	Mala datoteka koju je kreirala neka Web lokacija i snimila je na vaše računalo, a koristi se za skupljanje određenih informacija.
cryptography	kriptografija	Znanost o sigurnosti podataka, postupak skrivanja ili kodiranja informacija koje su pohranjene na nekom mjestu u računalnom sustavu ili se prenose e-poštom ili na neki drugi elektronički način.

Engleski pojam	Prijevod	Objašnjenje
decryption	dešifriranje	Postupak dekodiranja šifriranih podataka.
denial of service attack (DoS)	DoS napad	Napad koji poslužitelj opteretí velikim brojem zahtjeva za pružanjem usluga pa legitimni zahtjevi na dospiju biti zadovoljeni.
desktop monitoring program	program za nadziranje PC-a	*Spyware* program koji neovlašteno prati i bilježi sve operacije tuđeg računala.
dictionary attack	napad po rječniku	Napad po rječniku odnosi se na općenitu tehniku pokušaja pogađanja nečije tajne prolaskom kroz popis vjerojatnih mogućnosti, često popisa riječi iz rječnika. Ovaj napad uspijeva jer korisnici često imaju lozinke koje je lako pogoditi, iako ih se upozorava da u lozinkama koriste kombinacije brojki i slova.
dictionary spam	*spam* rječnik	Način pronalaženja adresa e-pošte spajanjem imena s poznatim imenima neke domene.
digital certificate	digitalni certifikat	Elektronička potvrda identiteta neke osobe, poslužitelja, davatelja usluga ili proizvođača softvera.
digital signature	digitalni potpis	Oblik digitalnog certifikata koji se koristi za provjeru vjerodostojnosti pošiljatelja neke poruke ili potpisnika nekog dokumenta.
DNS soopfing		Napad koji počinje otmicom DNS imena računala; DNS ime preusmjerava se na IP adresu napadača.
encryption	šifriranje	Postupak kodiranja podataka tako da ih, ako je šifriranje uspješno, ne može pročitati netko koji ih ne smije vidjeti.
exploit	iskorištavanje pukotina	Napad koji koristi bug ili 'pukotinu' u hardveru ili softveru operativnog sustava ili aplikacija.
firewall	vatrozid	Softver ili hardver koji računalo ili mrežu odvaja od Interneta.
Heuristic scanning	heurističko skeniranje	Metoda skeniranja virusa traženjem općih karakteristika virusa.
hoax	obmana	Lažne informacije o navodnom napadu virusa.
hybrid virus	hibridni virus	Virus koji kombinira različite karakteristike drugih vrsta virusa.
ICMP (Internet Control Message Protocol)	ICMP	Protokol koji koristi Internet usmjernik da bi obavijestio računalo-domaćina kako se do nekog odredišta ne može doći.

Engleski pojam	Prijevod	Objašnjenje
decryption	dešifriranje	Postupak dekodiranja šifriranih podataka.
denial of service attack (DoS)	DoS napad	Napad koji poslužitelj optereti velikim brojem zahtjeva za pružanjem usluge pa legitimni zahtjevi na dospiju biti zadovoljeni.
desktop monitoring program	program za nadziranje PC-a	*Spyware* program koji neovlašteno prati i bilježi sve operacije tuđeg računala.
dictionary attack	napad po rječniku	Napad po rječniku odnosi se na općenitu tehniku pokušaja pogađanja nečije tajne prolaskom kroz popis vjerojatnih mogućnosti, često popisa riječi iz rječnika. Ovaj napad uspijeva jer korisnici često imaju lozinke koje je lako pogoditi, iako ih se upozorava da u lozinkama koriste kombinacije brojki i slova.
dictionary spam	*spam* rječnik	Način pronalaženja adresa e-pošte spajanjem imena s poznatim imenima neke domene.
digital certificate	digitalni certifikat	Elektronička potvrda identiteta neke osobe, poslužitelja, davatelja usluga ili proizvođača softvera.
digital signature	digitalni potpis	Oblik digitalnog certifikata koji se koristi za provjeru vjerodostojnosti pošiljatelja neke poruke ili potpisnika nekog dokumenta.
DNS soopfing		Napad koji počinje otmicom DNS imena računala; DNS ime preusmjerava se na IP adresu napadača.
encryption	šifriranje	Postupak kodiranja podataka tako da ih, ako je šifriranje uspješno, ne može pročitati netko koji ih ne smije vidjeti.
exploit	iskorištavanje pukotina	Napad koji koristi bug ili 'pukotinu' u hardveru ili softveru operativnog sustava ili aplikacija.
firewall	vatrozid	Softver ili hardver koji računalo ili mrežu odvaja od Interneta.
Heuristic scanning	heurističko skeniranje	Metoda skeniranja virusa traženjem općih karakteristika virusa.
hoax	obmana	Lažne informacije o navodnom napadu virusa.
hybrid virus	hibridni virus	Virus koji kombinira različite karakteristike drugih vrsta virusa.
ICMP (Internet Control Message Protocol)	ICMP	Protokol koji koristi Internet usmjernik da bi obavijestio računalo-domaćina kako se do nekog odredišta ne može doći.

Engleski pojam	Prijevod	Objašnjenje
personal firewall	osobni vatrozid	Program vatrozida kreiran za kućni ili poslovni PC.
port scanner	skener portova	Program koji traži otvorene portove na tuđim računalima.
Pretty Good Privacy (PGP)	PGP	Jadan od najpopularnijih alata za javno šifriranje.
private key	privatni ključ	Tajni ključ koji se može upotrijebiti ili samostalno za šifriranje poruke ili s pridruženim javnim ključem za dešifriranje poruke šifrirane javnim ključem. Pripada kategoriji šifriranja po dva ključa.
proof of concept	dokaz koncepta	Virus koji je kreiran samo zato da bi se testirala postojanost nekog koncepta ili tehnologije.
public key	javni ključ	Ključ koji osigurava nadležno tijelo ili vlasnik privatnog ključa, koji se u kombinaciji s privatnim ključem može koristiti za dešifriranje šifrirane poruke. *Pogledajte* public key.
rootkit		Vrsta zlonamjernog softvera koji se aktivira svaki put kada se vaš sustav podiže. Taj se softver teško otkriva jer se aktivira prije nego što se vaš operativni sustav podigne u potpunosti, a omogućuje instaliranje skrivenih datoteka, procesa, skrivenih korisničkih računa u operativnom sustavu.
sandboxing		Proces pokretanja programa u izoliranom (ili virtualnom) području, čime se štiti računalo od eventualnih problema uzrokovanih zarazom virusom tijekom testiranja.
secure server	zaštićeni poslužitelj	Web poslužitelj koji koristi šifriranje za zaštitu korisničkih transakcija.
Secure Sockets Layer (SSL)	SSL	Oblik šifriranja koji se koristi za zaštitu poslužitelja.
session key	ključ sesije	Privremeni ključ koji se koristi za šifriranje ili dešifriranje neke poruke u trenutnoj računalnoj sesiji.
sniffer	snifer	Program koji se koristi za otkrivanje *online* dostupnosti računala.
social engineering attack	napad pomoću društvenog inženjeringa	Provala u sustav s na prijevaru dobivenim korisničkim podacima za prijavu (korisničko ime i lozinku).
spam		Nepoželjne poruke e-pošte koju mogu biti bezazlene i koristiti se za ciljano oglašavanje, ali mogu sadržavati i zlonamjerni kod.

Engleski pojam	Prijevod	Objašnjenje
spyware		Program koji se koristi za praćenje aktivnosti na nekom računalu bez znanja korisnika (špijuniranje korisnika).
symmetric key encryption	šifriranje simetričnim ključem	Način šifriranja podataka kod kojeg obje strane koje razmjenjuju informacije imaju pristup istom ključu.
tradecraft		Tehnika koju koriste špijuni za neprimjetno vođenje svojih poslova, na primjer, načini prosljeđivanja informacija od jednog agenta do drugog na prometnoj ulici.
Trojan horse	trojanski konj	Zlonamjerni program koji se u sustav uvlači pod okriljem nekog bezopasnog softvera ili datoteke.
virus	virus	Računalni program ili dio zlonamjernog koda koje se povezuje s nekom datotekom, a potom se razmnožava.
war driving	ratna vožnja	Vožnja po nekom dijelu grada s posebnom elektroničkom opremom u potrazi za nestabilnim ili nezaštićenim bežičnim mrežama.
worm	crv	Parazitski program koji se razmnožava ali ne inficira druge datoteke.

Sigurni na Internetu

Zaštitite se!

Jednostavan i sveobuhvatan praktični vodič od najpouzdanijeg proizvođača sigurnosnog softvera – Symanteca

Internet vrvi rizicima; ako obavljate novčane transakcije *online* ili samo pretražujete Web i šaljete e-poštu, izlažete se lopovima i prevarantima. Današnji "zločesti dečki" ne trebaju obijati vaše brave ni razbijati prozore: oni preko Interneta napadaju vas i vašu obitelj. Jeste li za to pripremljeni? S ovim Symantecovim vodičem uživajte u sigurnijem korištenju Interneta.

Ova lako razumljiva knjiga pomoći će vam da se zaštitite od prijetnji s Interneta i naučiti vas kako sebe i svoju obitelj štititi dok ste *online*.

- Očuvajte svoje računalo od *spywarea*, *adwarea*, crva, virusa i provalnika.
- Zaštitite svoj identitet i privatnost.
- Sigurno pretražujte Web i uklonite *spam* poštu iz svojeg poštanskog sandučića.
- Držite njuškala dalje od svoje bežične mreže.
- Iskoristite u najvećoj mogućoj mjeri nove sigurnosne značajke ugrađene u Windows XP.
- Zaštitite svoju djecu od pornografije i *online* grabežljivaca.
- Zaštitite svoju novu internetsku telefonsku uslugu.
- Preuzmite s Interneta besplatne alate koji će vam pomoći da štitite svoje računalo.

Andrew Conry-Murray, urednik za tehnologiju u *IT Architectu*, specijalizirao se u pisanju publikacija o sigurnosti na Internetu. Njegovi se radovi pojavljuju i u časopisima *Internet Week* i *Network Computing*.

Vincent Weafer, direktor Symantec Security Responsea, nadgleda tim stručnjaka za sigurnost koji istražuje nove prijetnje na Internetu da bi pružio najpouzdanije, brze informacije o trenutnim prijetnjama sigurnosti. Njegov tim pruža rješenja i usluge koje pomažu pojedincima i tvrtkama da osiguraju odgovarajuću zaštitu, dostupnost i integritet svojih informacija.

Addison Wesley

symantec. press

www.mis.hr

MIŠ

ISBN 953-6961-68-7

9 789536 961689